The Dissertation Committee for Kathleen Lizabeth Petersen
Certifies that this is the approved version of the following dissertation:

One-Cusped Congruence Subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$

Committee:

Alan Reid, Supervisor

Cameron Gordon

John Luecke

Daniel Allcock

Ted Chinburg

One-Cusped Congruence Subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$

by

Kathleen Lizabeth Petersen, B.A.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2005

Acknowledgments

First, I would like to express my gratitude to my advisor, Alan Reid, for his patience, support, and guidance. Thanks also go to my committee members Daniel Allcock, Ted Chinburg, Cameron Gordon, and John Luecke. Additionally, I would like to thank Felipe Voloch for bringing Artin's Primitive Root Conjecture to my attention. I also want to acknowledge John Hammond for assisting me with *Mathematica*.^{TM} Finally, thanks to my friends and family who helped me along the way.

One-Cusped Congruence Subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$

Publication No. _____

Kathleen Lizabeth Petersen, Ph.D.
The University of Texas at Austin, 2005

Supervisor: Alan Reid

Let K be a number field with r real places and s complex places, and let $\mathcal{O}_K$ be the ring of integers of K. The group $\mathrm{PSL}_2(\mathcal{O}_K)$ embeds discretely in $\mathrm{PSL}_2(\mathbb{R})^r \times \mathrm{PSL}_2(\mathbb{C})^s$, the group of orientation preserving isometries of $X_{r,s} = [\mathbb{H}^2]^r \times [\mathbb{H}^3]^s$, and acts with finite covolume. Hence for any finite index subgroup, Γ of $\mathrm{PSL}_2(\mathcal{O}_K)$, the quotient $[\mathbb{H}^2]^r \times [\mathbb{H}^3]^s/\Gamma$ is a finite volume $(2r + 3s)$-dimensional orbifold. The quotient $X_{r,s}/\mathrm{PSL}_2(\mathcal{O}_K)$ has h_K cusps, where h_K is the class number of $\mathcal{O}_K$, therefore the quotient by Γ has at least h_K cusps. Petersson proved that there are only finitely many congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ whose quotient has one cusp. We show that when K is an imaginary quadratic there are only finitely many maximal congruence subgroups whose quotient has one cusp. In contrast, under the assumption of the Generalized Riemann Hypothesis, we show that if K is neither $\mathbb{Q}$ nor an imaginary quadratic, and $i \notin K$ then there are infinitely many maximal congruence subgroups whose quotient has one cusp, relating this condition to a generalization of Artin's primitive root conjecture.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Overview and Statement of Results

Let K be a number field, that is, a finite extension of $\mathbb{Q}$, and let $\mathcal{O}_K$ be the ring of integers of K. The algebraic properties of the groups $\mathrm{PSL}_2(\mathcal{O}_K)$ and the geometric properties of their quotients have been studied extensively. In the context of low-dimensional topology, the cases in which K is $\mathbb{Q}$ or an imaginary quadratic number field are most relevant. The *Modular Group,* $\mathrm{PSL}_2(\mathbb{Z})$, embeds in $\mathrm{PSL}_2(\mathbb{R})$ discretely. As $\mathrm{PSL}_2(\mathbb{R})$ is isomorphic to the group of orientation preserving isometries of the hyperbolic plane, $\mathbb{H}^2$, we can form the quotient $\mathbb{H}^2/\mathrm{PSL}_2(\mathbb{Z})$. This quotient has finite volume as a hyperbolic 2-orbifold with a single cusp. The quotient $\mathbb{H}^2/\mathrm{PSL}_2(\mathbb{Z})$ is the prototype for non-compact arithmetic 2-orbifolds, which are defined as those orbifolds M such that $M \cong \mathbb{H}^2/\Gamma$ for some Γ that is commensurable with the Modular Group up to conjugacy. Similarly, let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{-d})$, where $d \in \mathbb{N}$ is square-free. The groups $\mathrm{PSL}_2(\mathcal{O}_d)$ are called the *Bianchi Groups* and they embed discretely in $\mathrm{PSL}_2(\mathbb{C})$. Since $\mathrm{PSL}_2(\mathbb{C}) \cong \mathrm{Isom}^+(\mathbb{H}^3)$, the quotient $M_d = \mathbb{H}^3/\mathrm{PSL}_2(\mathcal{O}_d)$ is a finite volume hyperbolic 3-orbifold. As in the case of the Modular Group, the quotients M_d are the prototypical examples of non-compact arithmetic 3-orbifolds. A *non-compact arithmetic 3-orbifold*

is an orbifold M such that $M \cong \mathbb{H}^3/\Gamma$ for some Γ commensurable up to conjugacy with a Bianchi Group.

In general, if K is a number field with r real places and s complex places, the group $\mathrm{PSL}_2(\mathcal{O}_K)$ embeds discretely in $\mathrm{PSL}_2(\mathbb{R})^r \times \mathrm{PSL}_2(\mathbb{C})^s$, the group of orientation preserving isometries of $X_{r,s} = [\mathbb{H}^2]^r \times [\mathbb{H}^2]^s$. The quotient $M_K = X_{r,s}/\mathrm{PSL}_2(\mathcal{O}_K)$ is equipped with a metric inherited from $[\mathbb{H}^2]^r \times [\mathbb{H}^3]^s$ and with respect to this metric M_K has finite volume. The orbifold M_K has h_K cusps, where h_K is the class number of $\mathcal{O}_K$. [27]

These groups and other matrix groups over number rings have been studied extensively, especially in the context of their normal subgroups. The most natural normal subgroups are the principal congruence subgroups defined as follows. For a non-zero ideal $J \subset \mathcal{O}_K$, the *principal congruence subgroup of level* J is

$$\Gamma(J) = \{M \in (\mathrm{P})\mathrm{SL}_n(\mathcal{O}_K) : M \equiv I \mod J\}.$$

A subgroup of $\mathrm{PSL}_n(\mathcal{O}_k)$ is called a *congruence subgroup* if it contains a principal congruence subgroup. We say that $\mathrm{PSL}_n(\mathcal{O}_K)$ has the *Congruence Subgroup Property (CSP)* if all finite index subgroups are congruence subgroups. It has been shown through an extensive series of results that $\mathrm{PSL}_n(\mathcal{O}_K)$ fails to have the CSP precisely when $n \geq 3$ and K is totally imaginary, or $n = 2$ and $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$ [20, 8, 15, 3, 23, 13]. Indeed one can refine this further, let $G = \mathrm{PSL}_n(\mathcal{O}_K)$ and define the profinite (resp. congruence) topology by specifying that the finite index (congruence) subgroups are a basis of neighborhoods of the identity. Let $\widehat{G}$ denote the profinite completion of G, and $\overline{G}$ to be the congruence completion of G. There is a $C(G)$ such that the following

sequence is exact, [3]

$$\{1\} \to C(G) \to \widehat{G} \to \overline{G} \to \{1\}.$$

We have defined G to have the CSP if $C(G)$ is trivial, that is, if $\widehat{G}$ is with $\overline{G}$. A more modern approach is to say that G has the CSP if $C(G)$ is finite. With this definition, $\mathrm{PSL}_n(\mathcal{O}_K)$ fails to have the CSP precisely when $n = 2$ and $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$. [23]

If Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ such that the quotient $X_{r,s}/\Gamma$ has n cusps we will say that Γ is *n-cusped.* In the case of surfaces, Rhode proved that there are at least two conjugacy classes of one-cusped subgroups of index n in the Modular Group for every positive integer n. [18] Later, Petersson proved that there are only finitely many one-cusped congruence subgroups of the Modular Group, and that the index of any such group divides $55440 = 11 \cdot 7 \cdot 5 \cdot 3^2 \cdot 2^4$. [19] Famously, the only $\mathcal{O}_d$ with class number one are $d = 1$, 2, 3, 7, 11, 19, 43, 67, and 163. Of these, only when $d = 1$, 2, 3, 7, or 11 is $\mathcal{O}_d$ a Euclidean Domain, with respect to the Euclidean Algorithm or any other function. [16] Hence by our previous discussion, the values of d such that $\mathcal{O}_d$ has class number one are the only values for which $\mathrm{PSL}_2(\mathcal{O}_d)$ can contain a one-cusped subgroup. In contrast, it is a famous conjecture that there are infinitely many real quadratics with class number equal to one.

Reid [21] showed that the figure-eight knot is the only arithmetic knot complement in S^3. The fundamental group of the figure-eight knot complement injects into $\mathrm{PSL}_2(\mathcal{O}_3)$ as an index 12 subgroup. Moreover, it is a congruence subgroup containing $\Gamma(4)$. [11] The fundamental group of the sister of the figure-eight knot complement, a knot in $L(5,1)$, also injects into $\mathrm{PSL}_2(\mathcal{O}_3)$

as an index 12 subgroup and contains $\Gamma(2)$. [2] If $d \neq 1$ or 3, there are infinitely many one-cusped subgroups (not necessarily torsion-free) since there is a surjection from $\mathrm{PSL}_2(\mathcal{O}_d)$ onto $\mathbb{Z}$, with a parabolic element generating the image. If $d = 1$ or 3 there are also infinitely many one-cusped subgroups, associated to torsion-free subgroups of finite index, e.g. subgroups of finite index in the fundamental group of the figure-eight knot complement. [4] But it is still unknown whether or not there are infinitely many maximal one-cusped subgroups of the Bianchi Groups. There are examples of torsion-free one-cusped subgroups of $\mathrm{PSL}_2(\mathcal{O}_d)$ corresponding to d =1, 2, 3, 7, and 11. [4, 2, 1] In the setting of arithmetic manifolds and orbifolds, it has recently been shown that there is a finite number of commensurability classes of one-cusped orbifolds or manifolds of minimal volume. [6]

Our first main result is the following generalization of Petersson's result.

Theorem 1.1.1. *There are finitely many maximal one-cusped congruence subgroups of the Bianchi groups.*

We can say more. To explain this we introduce a useful invariant of finite index subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$ is the level of the group which has added meaning for congruence subgroups.

Definition 1.1.1. Let $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$. We say that Γ has $\mathcal{O}_K$-*level* L if L is an ideal in $\mathcal{O}_K$ maximal with respect to the property that the normal closure of the group generated by the elements

$$\left\{ \pm \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} : l \in L \right\}$$

is contained in Γ. Moreover, we say that Γ has $\mathbb{Z}$-*level* n if n is the smallest positive integer such that the normal closure of the group generated by the elements

$$\left\{ \pm \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix} : \nu \in n\mathcal{O}_K \right\}$$

is contained in Γ.

We show that any prime in $\mathcal{O}_d$ that divides the $\mathbb{Z}$-level of a one-cupsed congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ has norm less than or equal to 11. If $d =$ 11, 19, 43, 67, or 163 we can prove the exact analog of Petersson's result, that there are only **finitely many** one-cusped congruence subgroups. The methods used will result in explicit bounds for the maximal power of a prime that can divide the $\mathbb{Z}$-level. In addition, if $d =$ 1,2, or 7, we show that there are finitely many of odd $\mathbb{Z}$-level, and if $d = 3$ we demonstrate that there are finitely many of $\mathbb{Z}$-level relatively prime to 21. Moreover, a corollary of our methods gives stronger information in the torsion-free setting. Namely,

Corollary 1.1.2. *If* $d = 19, 43, 67,$ *or* 163 *there are no torsion-free one-cusped congruence subgroups of* $\mathrm{PSL}_2(\mathcal{O}_d)$.

By way of contrast, which is reflective of the dichotomy of the CSP mentioned earlier

Theorem 1.1.3. *Let* K *be a number field with class number one other than* $\mathbb{Q}$ *or an imaginary quadratic, such that* $i \notin K$. *Assuming the Generalized Riemann Hypothesis, there are infinitely many maximal one-cusped congruence subgroups of* $\mathrm{PSL}_2(\mathcal{O}_K)$.

In a different direction,

Theorem 1.1.4. *Let K be $\mathbb{Q}$ or an imaginary quadratic number field with class number one. There are infinitely many maximal congruence subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$ that have two cusps. Moreover, for any even integer n, there are infinitely many primes $\mathcal{P} \subset \mathcal{O}_K$ such that there is an n-cusped congruence subgroup of $\mathcal{O}_K$-level $\mathcal{P}$.*

1.2 Number Theory

In this section we will review some number theory. Our references are [26] and [14]. If K is a number field, it is necessarily a simple extension, so $K = \mathbb{Q}(\alpha)$ where α is the root of a monic, irreducible polynomial $f(x) \in \mathbb{Q}[x]$. This is the minimal polynomial for α over $\mathbb{Q}$. The degree, d, of f equals the degree of the extension K over $\mathbb{Q}$, and f has d roots, $\alpha_1, \ldots, \alpha_d$ which are necessarily distinct. The mapping $\alpha_i \to \alpha_j$ induces an isomorphism $\mathbb{Q}(\alpha_i) \to \mathbb{Q}(\alpha_j)$. Any embedding of $K \to \mathbb{C}$ occurs in this way, so there are exactly d embeddings of K in $\mathbb{C}$. Let $\sigma_1, \ldots, \sigma_d$ be these embeddings, where σ_i corresponds to the mapping from $K = \mathbb{Q}(\alpha_1)$ to $\mathbb{Q}(\alpha_i)$. Since f has rational coefficients, the roots α_i are either in $\mathbb{R}$, or occur as complex conjugate pairs. The corresponding embeddings $\sigma_i(K)$ will be contained in $\mathbb{R}$ exactly when $\alpha_i \in \mathbb{R}$. If K has r real embeddings and s pairs of complex conjugate embeddings, then $d = r + 2s$. We say that K has r *real places* and s *complex places.* For any $\alpha \in K$, we define the *norm* of α, as

$$N_{K|\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_d(\alpha).$$

This is (up to sign) the constant of the minimal polynomial for α over $\mathbb{Q}$.

An element $\alpha \in \mathbb{C}$ is an *algebraic integer,* or simply an *integer,* if α satisfies a monic polynomial with coefficients in $\mathbb{Z}$. As a result, if α is an algebraic integer, $N_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$. For clarity, an element of $\mathbb{Z}$ will often be called a rational integer. By Gauss's Lemma, the minimal polynomial for α must also be monic. The additive ring $\mathbb{Z}[\alpha]$ is finitely generated when α is an integer, and so the set of algebraic integers in $\mathbb{C}$ forms a ring. For a number field K, the set of algebraic integers in K forms a ring and will be denoted $\mathcal{O}_K$, the *ring of integers of* K. In the case where $K = \mathbb{Q}[\sqrt{-d}]$ for d a square-free positive integer, we will use the shorthand $\mathcal{O}_d$ for $\mathcal{O}_K$. Furthermore,

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{-d}] & \text{if } d \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{-d}}{2}] & \text{if } d \equiv 1 \mod 4. \end{cases}$$

An integral domain is called a *Dedekind domain* if every non-zero proper ideal of D can be written as a finite product of (not necessarily distict) prime ideals. This set of primes is uniquely determined, and every non-zero proper ideal can be written uniquely (up to order) as a product of powers of prime ideals. If A and B are ideals in an integral domain D, we say that B divides A if there is an ideal C in D where $A = BC$. For an integral domain D, and an element $a \in D$, we use the notation (a) to represent the principal ideal aD. Moreover, if $a_1, a_2, \ldots a_n \in D$, $(a_1, a_2, \ldots a_n)$ is the ideal generated by the elements a_i for $1 \leq i \leq n$. The ring of integers of a number field is a Dedekind domain. For a non-zero ideal I of $\mathcal{O}_K$, $\mathcal{O}_K/I$ is a finite ring, and we define the *norm* of I as $N(I) = |\mathcal{O}_K/I|$. The norm is multiplicative, if I and J are nonzero ideals, $N(IJ) = N(I)N(J)$.

If $\mathcal{P}$ is a non-zero prime ideal then $\mathcal{O}_K/\mathcal{P} \cong \mathbb{F}_q$ where $q = p^k$ for a prime p in $\mathbb{Z}$. The exponent f is called the *inertial degree* of $\mathcal{P}$. If $p \in \mathbb{Z}$ is a prime

and $\mathcal{P}$ is a prime ideal in $\mathcal{O}_K$ such that $p\mathcal{O}_k \subset \mathcal{P}$, then we say that $\mathcal{P}$ *lies over* p, and p *lies under* $\mathcal{P}$.Therefore p lies under $\mathcal{P}$ precisely when $N(\mathcal{P}) = p^k$. For a prime $p \in \mathbb{Z}$, there are unique primes $\mathcal{P}_i \subset \mathcal{O}_K$ such that

$$p\mathcal{O}_K = \mathcal{P}_1^{e_1} \dots \mathcal{P}_s^{e_s}.$$

The exponent e_i is called the *ramification index* of $\mathcal{P}_i$, and we say that p is *ramified* in K if there is an $e_i > 1$. If f_i is the inertial degree of $\mathcal{P}_i$ then

$$[K : \mathbb{Q}] = \sum_{i=1}^{s} e_i f_i.$$

Since we will make extensive use of the case where $K = \mathbb{Q}[\sqrt{-d}]$ in the proof of Theorem 1.1.1, and Theorem 1.1.4 we will discuss it in more detail. There are three possibilities for the decomposition of an ideal $p\mathcal{O}_d$ when p is a rational prime.

$$p\mathcal{O}_d = \begin{cases} \mathcal{P}^2 & \text{we say } p \text{ is } \textit{ramified} \\ \mathcal{P} & \text{we say } p \text{ is } \textit{inert} \\ \mathcal{P}_1\mathcal{P}_2 & \text{we say } p \text{ is } \textit{split}. \end{cases}$$

This behavior can be completely classified. The prime p is ramified exactly when p divides the discriminant of $\mathbb{Q}[\sqrt{-d}]$,

$$disc(\mathbb{Q}[\sqrt{-d}]) = \begin{cases} d & \text{if } -d \equiv 1 \mod 4 \\ 4d & \text{if } -d \not\equiv 1 \mod 4. \end{cases}$$

If $p = 2$ we have the following decomposition

$$2\mathcal{O}_d = \begin{cases} (2, 1+\sqrt{-d})^2 & \text{if } 2|d \text{ or } -d \not\equiv 1 \mod 4 \\ (2, \frac{1+\sqrt{-d}}{2})(2, \frac{1-\sqrt{-d}}{2}) & \text{if } -d \equiv 1 \mod 8 \\ (2) & \text{if } -d \equiv 5 \mod 8, \end{cases}$$

and if p is odd, we have

$$p\mathcal{O}_d = \begin{cases} (p, \sqrt{-d})^2 & \text{if } p|d \\ (p, n+\sqrt{-d})(p, n-\sqrt{-d}) & \text{if } \exists n \text{ such that } -d \equiv n^2 \mod p \\ (p) & \text{otherwise.} \end{cases}$$

If p is not inert and $\mathcal{P}$ lies over p, then $\mathcal{O}_d/\mathcal{P} \cong \mathbb{F}_p$ and $N(\mathcal{P}) = p$. If p is inert then $p\mathcal{O}_d = \mathcal{P}$, $\mathcal{O}_d/\mathcal{P} \cong \mathbb{F}_{p^2}$ and $N(\mathcal{P}) = p^2$.

A fractional ideal of $\mathcal{O}_K$ is a set of the form aI for some $a \in K$ and some ideal I of $\mathcal{O}_K$. Let K be a number field, and I_K be the group of non-zero fractional ideals of $\mathcal{O}_K$. The group I_K is called the *ideal group* of K. Let P_K be the group of non-zero principal ideals of $\mathcal{O}_K$. We form the quotient I_K/P_K, the *class group* of K. This has finite order, and we call the order of the class group the *class number* of K. Clearly, the class number is one exactly when $\mathcal{O}_K$ is a PID. In the case of imaginary quadratic number fields, $\mathcal{O}_d$ has class number one precisely when

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

In contrast, it is conjectured that there are infinitely many real quadratic number fields with class number one.

Table 1.1:
Splitting Types of Small Primes in $\mathcal{O}_d$, R=Ramified, S=Split and I=Inert

	$d=1$	2	3	7	11	19	43	67	163
$p=2$	R	R	I	S	I	I	I	I	I
3	I	S	R	I	S	I	I	I	I
5	S	I	I	I	S	S	I	I	I
7	I	I	S	R	I	S	I	I	I
11	I	S	I	S	R	S	S	I	I

The ring of integers, $\mathcal{O}_K$, of a number field K is a free abelian group of rank d, where $d = [K : \mathbb{Q}]$. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an *integral basis* for K. Every number field has an integral basis. Let $\mathcal{O}_K^\times$ denote the multiplicative group of units in $\mathcal{O}_K$. The units are precisely those elements of norm ± 1. The

group $\mathcal{O}_K^\times$ is a direct product of a finite cyclic group, which consists of roots, and a free abelian group. The rank of the free abelian group is $r + s - 1$, where r is the number of real places of K and s is the number of complex places. A set of $r + s - 1$ generators for the free abelian factor is called a *fundamental set of units* for $\mathcal{O}_K$. If $\{u_1, u_2, \ldots, u_{r+s-1}\}$ is a set of fundamental units for $\mathcal{O}_K^\times$, every unit in $\mathcal{O}_K^\times$ can be uniquely written as $\zeta u_1^{a_1} u_2^{a_2} \ldots u_{r+s-1}^{a_{r+s-1}}$ where ζ is a root of unity. Thus $\mathcal{O}_K^\times$ is finite only when $K = \mathbb{Q}$ or an imaginary quadratic number field. When $K = \mathbb{Q}[\sqrt{-d}]$ the multiplicative group of units is simply ± 1 unless $d = 3$, or 1, when it also contains $(\pm 1 \pm \sqrt{-3})/2$ and $\pm i$, respectively.

If $\mathcal{P}$ is a prime in K and L/K is Galois then we define the *Frobenius Symbol* $(\mathcal{P}, L/K)$ to be the set of $\sigma \in Gal(L/K)$ such that there is a prime $Q \in L$ lying over $\mathcal{P}$ with $\sigma(\mathcal{Q}) = \mathcal{Q}$ and $\sigma(\alpha) \equiv \alpha^{N(\mathcal{P})} \mod \mathcal{Q}$. This defines a non-empty subset of $Gal(L/K)$ and if $\mathcal{P}$ is unramified it uniquely defines a conjugacy class. [12]

We will make use of the Čebotarev Density Theorem in the proof of Wohlfahrt's Theorem. Our reference for the following discussion is [26]. For a set S of prime ideals in $\mathcal{O}_K$, we define the *Dirichlet density* of S to be

$$\lim_{s \to 1} \left(\frac{\sum_{\mathcal{P} \subset S} N(\mathcal{P})^{-s}}{\sum_{\mathcal{P} \subset S_0} N(\mathcal{P})^{-s}} \right)$$

where S_0 is the set of prime ideals in $\mathcal{O}_K$. The Čebotarev Density Theorem is a generalization of Dirichlet's theorem on primes in an arithmetic progression, which states that if $m > 2$ and $(m, c) = 1$ then the primes p which satisfy $p \equiv c \mod m$ have Dirichlet density $\phi(m)^{-1}$, where ϕ is Euler's function.

Before we state the theorem, we will define the congruence divisor class group of K. Let m be the formal product of an integral ideal in K and a set (possibly empty) of real places in K, so $m = \prod p_\nu^{n_\nu}$. Let K_{p_μ} be the completion of K at p_μ. Let A_m be the subset of I_K consisting of all fractional ideals whose factorization does not contain any primes dividing m. Let H_m^0 be the subgroup of A_m consisting of principal ideals that can be written as (α) for some $\alpha \equiv 1 \mod m$, that is, $\alpha \equiv 1 \mod p_\mu^{n_\nu}$ in K_{p_μ} for each finite prime dividing m, and such that $\sigma(\alpha) > 0$ for the embeddings associated to infinite primes dividing m. The quotient A_m/H_m^0 is finite. For all such m, there is one equivalence class, A/H, of such A_m/H_m^0, and it is called the *congruence divisor class group.*

The Čebotarev Density Theorem states

Theorem 1.2.1. *Let K be a number field and A/H a congruence divisor class group in K. Let $\mathcal{C}$ be a coset of H in A. Then the Dirichlet density of the prime ideals in $\mathcal{C}$ is N^{-1}, where $N = \mathrm{card}(A/H)$.*

Let $m \in \mathcal{O}_K$ be non-zero and a_m relatively prime to m. As above, we think of m as a formal product of integral ideals in K and possibly some real infinite places of K, so $m = \prod p_\nu^{n_\nu}$. As a result $(a_m) \in A_m$. Let $\mathcal{C}$ be a coset of H in A, so $\mathcal{C} = aH$ for some $a \in A$. Then an equivalence class representative for A/H is A_m/H_m, where H_m is any subgroup of A_m that contains H_m^0. Since $\mathcal{C} = aH$, under this correspondence, $\mathcal{C} \leftrightarrow a_m H_m^0$ for some such a_m. Look at a prime $\mathcal{P}$ in $\mathcal{C}$. Since the class number of the $\mathcal{O}_K$ in consideration is 1, $\mathcal{P}$ is principal, therefore $\mathcal{P} = (p) = (a_m h)$ for some $h \in H_m^0$. Since $h \equiv 1 \mod m$, $p \equiv a_m \mod m$. Therefore, given a, b with $(a, b) = 1$ and a non-zero $k \in \mathcal{O}_K$,

for all primes $\mathcal{P} = (p) \subset \mathcal{C}$, where $\mathcal{C} \leftrightarrow aH_b$ we have $p \equiv a \mod b$, implying that there is an x such that $bx = p - a$, so $a + bx = p$. By Theorem 1.2.1 there are infinitely many such $\mathcal{P}$. Choosing Px such that $N(\mathcal{P}) > N(k)$ we see that $(a + xb, k) = 1$. We have shown

Corollary 1.2.2. *If $\mathcal{O}_K$ is a PID and if $a, b \in \mathcal{O}_K$ such that $(a, b) = 1$ then for any non-zero $k \in \mathcal{O}_K$ there is an $x \in \mathcal{O}_K$ such that $(a + bx, k) = 1$.*

1.3 The Groups $\mathrm{PSL}_2(\mathcal{O}_K)$

Let K be a number field with r real places and s complex conjugate places. If K is not $\mathbb{Q}$ or an imaginary quadratic number field then $(\mathrm{P})\mathrm{SL}_2(\mathcal{O}_K)$ is not a discrete subgroup of $(\mathrm{P})\mathrm{SL}_2(\mathbb{C})$, but it is discrete in a product of copies of $(\mathrm{P})\mathrm{SL}_2(\mathbb{R})$ and $(\mathrm{P})\mathrm{SL}_2(\mathbb{C})$. Let

$$\psi : (\mathrm{P})\mathrm{SL}_2(\mathcal{O}_K) \to (\mathrm{P})\mathrm{SL}_2(\mathbb{R})^r \times (\mathrm{P})\mathrm{SL}_2(\mathbb{C})^s$$

be defined by mapping

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \times_g \begin{pmatrix} g(a) & g(b) \\ g(c) & g(d) \end{pmatrix}$$

where the product is taken over all places, g. The image, $\psi((\mathrm{P})\mathrm{SL}_2(\mathcal{O}_K))$ is discrete in $(\mathrm{P})\mathrm{SL}_2(\mathbb{R})^r \times (\mathrm{P})\mathrm{SL}_2(\mathbb{C})^s$. Moreover, $M_K = [\mathbb{H}^2]^r \times [\mathbb{H}^3]^s / \mathrm{PSL}_2(\mathcal{O}_K)$ is equipped with a metric inherited from $[\mathbb{H}^2]^r \times [\mathbb{H}^3]^s$, and with respect to this metric has finite volume.

For a non-zero ideal $J \subset \mathcal{O}_K$, $(\mathrm{P})\mathrm{SL}_2(\mathcal{O}_K)/\Gamma(J) \cong (\mathrm{P})SL_2(\mathcal{O}_K/J)$. If the class number of $\mathcal{O}_K$ is one, we have the following structure. Let n, n_1 and n_2 be non-zero elements in $\mathcal{O}_K$ such that $(n) = (n_1) \cap (n_2)$ and $(n_1, n_2) = \mathcal{O}_K$,

then [17]

$$\mathrm{SL}_2(\mathcal{O}_K)/\Gamma(n) \cong \mathrm{SL}_2(\mathcal{O}_k/(n_1)) \times \mathrm{SL}_2(\mathcal{O}_K/(n_2)).$$

If $\mathcal{P}$ is a prime ideal, then $\mathcal{O}_K/\mathcal{P} \cong \mathbb{F}_{N(\mathcal{P})}$, the finite field with $N(\mathcal{P})$ elements, and therefore $(\mathrm{P})\mathrm{SL}_2(\mathcal{O}_K)/\Gamma(\mathcal{P}) \cong (\mathrm{P})\mathrm{SL}_2(\mathbb{F}_{N(\mathcal{P})})$. Given a non-zero $J \subset \mathcal{O}_K$, we can write $J = \mathcal{P}_0^{\nu_0} \dots \mathcal{P}_s^{\nu_s}$ where $\mathcal{P}_i$ is a prime for $0 \leq i \leq s$ and if $i \neq j$ then $\mathcal{P}_i \neq \mathcal{P}_j$. It can be shown that [17]

$$[\mathrm{SL}_2(\mathcal{O}_K) : \Gamma(J)] = \prod_{i=1}^{s} N(\mathcal{P}_i)^{3\nu_i} \left(1 - \frac{1}{N(\mathcal{P}_i)^2}\right).$$

1.4 Peripheral Subgroups

If Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ then M_Γ has finite volume and

$$\mathrm{Vol}(M_\Gamma) = [\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]\mathrm{Vol}(M_K).$$

Recall that $\pm A \in \mathrm{PSL}_2(\mathbb{C})$ is parabolic if $\pm A \neq \pm I$ and $|\mathrm{trace}A| = 2$. We define $c \in \mathbb{C} \cup \infty$ to be a *cusp* of M_Γ if c is a parabolic fixed point of Γ, that is if there is some parabolic $A \in \Gamma$ such that

$$A = \pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

and

$$\frac{\alpha c + \beta}{\gamma c + \delta} = c.$$

For a cusp c we define

$$\mathrm{Stab}_c(\Gamma) = \left\{ \pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma : \frac{\alpha c + \beta}{\gamma c + \delta} = c \right\}.$$

In particular, $\mathrm{Stab}_\infty(\Gamma)$ consists of matrices of the form $\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}$. Two cusps are equivalent if they are in the same Γ orbit. As such, the number

of equivalence classes is the number of conjugacy classes of maximal peripheral subgroups of Γ, subgroups of the form $\mathrm{Stab}_c(\Gamma)$. This is the number of topological ends of M_Γ. The orbifold M_K has h_K cusps where h_K is the class number of K.

We will be particularly interested in those subgroups with the same number of cusps as $\mathrm{PSL}_2(\mathcal{O}_K)$.

Lemma 1.4.1. *Let K be a number field with class number h_K and Γ be a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$. If Γ has h_K cusps then*

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)].$$

Alternatively, if $h_K = 1$ and

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)]$$

then Γ has 1 cusp.

Proof. The covering of M_K by M_Γ induces a covering of the same degree of truncated compact orbifolds M'_K and M'_Γ. This cover restricts to a cover of $\partial M'_K$ by $\partial M'_\Gamma$. The degree of the cover of M'_K by M'_Γ is the degree of the cover of the cusp at infinity of M'_K by those cusps of $\partial M'_\Gamma$ covering it. If Γ has h_K cusps, then as $\mathrm{PSL}_2(\mathcal{O}_K)$ also has h_K cusps, the cusp at infinity of M'_Γ is the only cusp covering the cusp at infinity of M'_K. Therefore this covering degree, which is

$$[\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)]$$

is the degree of the cover of M_Γ to M_K which is $[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]$.

As remarked above, the degree of the cover of M_K by M_Γ, $[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]$, is the degree of the cover of the cusp at infinity of M'_K by those cusps of $\partial M'_\Gamma$ covering it. If

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)]$$

then only the cusp at infinity of M'_Γ can cover the cusp at infinity of M'_K. If $h_K = 1$ then M_K only has one cusp and so M_Γ has only one cusp as well.

□

Let K be a number field other than $\mathbb{Q}$ or an imaginary quadratic, and let $[K : \mathbb{Q}] = k$. Let r denote the number of real places of K, and s the number of complex places. Then we have seen that $\mathcal{O}_K^\times$ is isomorphic to $\mathbb{Z}^{r+s-1} \times \mathbb{Z}_t$ for some $t \in \mathbb{N}$. Let $\{u_1, u_2, \ldots u_{r+s-1}\}$ be a fundamental set of generators for $\mathcal{O}_K^\times$, and ζ be a primitive root of unity in $\mathcal{O}_K^\times$. Also, let $\{\omega_1, \omega_2, \ldots, \omega_k\}$ be an integral basis for K. Then $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K))$ is generated by elements of the form

$$\pm \begin{pmatrix} 1 & \omega_i \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} u_j & 0 \\ 0 & u_j^{-1} \end{pmatrix}, \text{and} \pm \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

where $1 \leq i \leq r+s-1$ and $i \leq j \leq k$. And $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K))$ consists of elements of the form

$$\pm \begin{pmatrix} \alpha & x \\ 0 & \alpha^{-1} \end{pmatrix}$$

for $\alpha \in \mathcal{O}_K^\times$ and $x \in \mathcal{O}_K$.

For $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$ let

$$\Lambda(\Gamma) = \left\{ x \in \mathbb{C} : \pm \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \Gamma \right\},$$

which is an abelian group. Moreover, $\Lambda(\Gamma)$ is a subgroup of $\Lambda(\mathrm{PSL}_2(\mathcal{O}_K)) = \mathcal{O}_K$. If K has class number one, we say that a cusp c of Γ has *width* w if after conjugating Γ in $\mathrm{PSL}_2(\mathcal{O}_K)$ so that the image of c is ∞, $[\Lambda(\mathrm{PSL}_2(\mathcal{O}_K)) : \Lambda(\Gamma)] = w$. If $c = \infty$ we will commonly use the notation $|\Lambda(\Gamma)|$ for the width of ∞.

Now we will look at $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K))$ in more detail. If $K = \mathbb{Q}$, then $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{Z}))$ is generated by $\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

In the case of imaginary quadratic number fields, $\mathcal{O}_d$ is discrete in $\mathbb{C}$. Let $\{1, \omega\}$ be an integral basis for $\mathcal{O}_d$. If $d \neq 1$ or 3 the only roots of unity in $\mathcal{O}_d$ are ± 1. The fourth roots of unity are in $\mathcal{O}_1$, generated by i, and the sixth roots of unity are in $\mathcal{O}_3$ generated by $(1 + \sqrt{-3})/2$. If $d \neq 1$ or 3,

$$\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_d)) = \left\langle \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix} \right\rangle$$

and geometrically, a cusp of M_d is $T \times [0, \infty)$ where T is a torus. If $\Lambda(\Gamma)$ has basis $\{a + ib, \alpha + i\beta\}$ then $|\Lambda(\Gamma)|$ is also $|a\beta - b\alpha|/|\mathrm{Im}\omega|$. If $d = 2$, 7, 11, 19,43, 67, or 163, $M_\Gamma = \mathbb{H}^3/\Gamma$ has one cusp, and the degree of the covering of M_d by M_Γ, $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma]$, is also the ratio of $|\Lambda(\Gamma)|$ to $|\Lambda(\mathrm{PSL}_2(\mathcal{O}_d))|$. To see this, recall that by Lemma 1.4.1 that

$$[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = [\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)]$$

and since $d \neq 1$ or 3, the stabilizers of infinity consist only of matrices of the form

$$\pm \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

which are in one to one correspondence with elements $x \in \Lambda$. Therefore, if Γ has one cusp,

$$[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = |\Lambda(\Gamma)|.$$

If $d = 1$, M_1 has a pillow cusp, the cusp is geometrically $S \times [0, \infty)$ where S is the 2-sphere with four cone points with cone angles π. And

$$\mathrm{Stab}_\infty(M_1) = \left\langle \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\rangle.$$

Elements of the form $\left(\pm \begin{matrix} -i & x \\ 0 & i \end{matrix} \right)$ for any $x \in \mathbb{Z}[i]$, have order two. If $\Gamma < \mathrm{PSL}_2(\mathcal{O}_1)$ has one cusp, and if $\mathrm{Stab}_\infty(\Gamma)$ contains torsion, then $[\mathrm{PSL}_2(\mathcal{O}_1) : \Gamma] = |\Lambda(\Gamma)|$. If Γ has one cusp and a torsion-free stabilizer at infinity, then $[\mathrm{PSL}_2(\mathcal{O}_1) : \Gamma] = 2|\Lambda(\Gamma)|$.

If $d = 3$, the cusp of M_3 is geometrically $S \times [0, \infty)$ where S is a sphere with 3 cone points of cone angles $2\pi/3$. And

$$\mathrm{Stab}_\infty(M_3) = \left\langle \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix} \right\rangle$$

where

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

Elements of the form $\pm \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$ have order 3. As in the $\mathcal{O}_1$ case, if $\Gamma < \mathrm{PSL}_2(\mathcal{O}_3)$ has one cusped, and if $\mathrm{Stab}_\infty(\Gamma)$ contains torsion, then $[\mathrm{PSL}_2(\mathcal{O}_3) : \Gamma] = |\Lambda(\Gamma)|$. If Γ has a torsion-free stabilizer at infinity, then $[\mathrm{PSL}_2(\mathcal{O}_3) : \Gamma] = 3|\Lambda(\Gamma)|$.

Definition 1.4.1. Let Γ be a one-cusped subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ then $T(\Gamma) \in \{1, 2, 3\}$ is the number such that $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T|\Lambda(\Gamma)|$.

Therefore

$$T(\Gamma) = \begin{cases} 1 & \text{if } d = 2, 3, 7, 11, 43, 67, 163 \\ 1 & \text{if } d = 1, 3 \text{ and } \Gamma \text{ has peripheral torsion} \\ 2 & \text{if } d = 1 \text{ and } \Gamma \text{ has no peripheral torsion} \\ 3 & \text{if } d = 3 \text{ and } \Gamma \text{ has no peripheral torsion.} \end{cases}$$

Chapter 2

Proof of Theorem 1.1.3

We will prove that if K is a number field other than $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$ that has class number one and $i \notin K$ then assuming the Generalized Riemann Hypothesis, there are infinitely many maximal one-cusped congruence subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$.

Assumption: *For all square-free $n > 0$ the Dedekind zeta function of $K(\zeta_n, (\mathcal{O}_K^\times)^{1/n})$ satisfies the generalized Riemann Hypothesis, where ζ_n is a primitive n^{th} root of unity. [12]*

Let $k = [K : \mathbb{Q}]$, and let $\{\omega_1 \dots \omega_k\}$ be an integral basis for $\mathcal{O}_K$. Let $\{f_j\}$ be a fundamental system of generators for $\mathcal{O}_K^\times$ for $1 \leq j \leq r+s-1$. If there is a $\mathbb{Z}/t\mathbb{Z}$ factor, let f_{r+s} correspond to a generator. Let $M = r+s$ in this case, and $r+s-1$ if there is no $\mathbb{Z}/t\mathbb{Z}$ factor. Therefore

$$\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) = \left\{ \pm \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \in \mathcal{O}_K^\times, \beta \in \mathcal{O}_K \right\}$$

and is generated by elements of type

$$\pm \begin{pmatrix} 1 & \omega_i \\ 0 & 1 \end{pmatrix}, \text{and} \pm \begin{pmatrix} f_j & 0 \\ 0 & f_j^{-1} \end{pmatrix}$$

for $1 \leq j \leq M$ and $1 \leq i \leq k$.

Let $\mathcal{P}$ be a non-zero prime ideal in $\mathcal{O}_K$ and $q = N(\mathcal{P})$. Recall that $\mathcal{O}_K/\mathcal{P} \cong \mathbb{F}_q$ and the multiplicative group of non-zero residue classes modulo $\mathcal{P}$, $(\mathcal{O}_K/\mathcal{P})^\times$, is isomorphic to $\mathbb{F}_q^\times \cong \mathbb{Z}_{q-1}$. Let $U_\mathcal{P}$ denote the reduction of $\mathcal{O}_K^\times$ modulo $\mathcal{P}$, $U_\mathcal{P} = \mathcal{O}_K^\times/(\mathcal{P} \cap \mathcal{O}_K^\times)$. Therefore we can think of $U_\mathcal{P}$ as a subgroup of $(\mathcal{O}_K/\mathcal{P})^\times$. Let

$$\phi_\mathcal{P} : \mathrm{PSL}_2(\mathcal{O}_K) \to \mathrm{PSL}_2(\mathbb{F}_q)$$

be the reduction modulo $\mathcal{P}$ map.

Recall that by Lemma 1.4.1 that if Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ such that

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)]$$

then Γ has one cusp.

We will use the following lemma, which we will defer the proof of until after we have completed the proof of Theorem 1.1.3.

Lemma 2.0.1. *Assuming the GRH if K is as above, then there are infinitely many primes $\mathcal{P}$ in $\mathcal{O}_K$ with $N(\mathcal{P}) \equiv 3 \mod 4$ such that $\mathcal{O}_K^\times$ surjects $\mathbb{F}_q^\times$ under the modulo $\mathcal{P}$ map, i.e. such that $\mathcal{O}_K^\times/(\mathcal{P} \cap \mathcal{O}_K^\times)$ coincides with $(\mathcal{O}_K/\mathcal{P})^\times$.*

We will assume that $\mathcal{P}$ is as in Lemma 2.0.1. By the classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ [25], there is a subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$ isomorphic to D_{q+1}, the dihedral group of order $q+1$. Since $|\mathrm{PSL}_2(\mathbb{F}_q)| = \frac{1}{2}q(q^2-1)$, the index of D_{q+1} is $\frac{1}{2}q(q-1)$. Let

$$\Gamma = \phi_\mathcal{P}^{-1}(D_{q+1}).$$

We will show that Γ has one cusp by demonstrating that one can choose all coset representatives for Γ in $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K))$. Since the $\mathcal{O}_K$-level of

$\phi_{\mathcal{P}}^{-1}(D_{q+1})$ is $\mathcal{P}$, this will prove that there are infinitely many maximal one-cusped congruence subgroups.

First, we will show that one can choose all coset representatives for D_{q+1} in $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$ where

$$\mathrm{Stab}_\infty((\mathrm{P})\mathrm{SL}_2(\mathbb{F}_q)) = \left\{(\pm)\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in (\mathrm{P})\mathrm{SL}_2(\mathbb{F}_q)\right\}.$$

For every choice of $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$ we have a unique matrix, $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ in $\mathrm{Stab}_\infty(\mathrm{SL}_2(\mathbb{F}_q))$. As $|\mathbb{F}_q| = q$ and $|\mathbb{F}_q^\times| = q-1$ we conclude that

$$|\mathrm{Stab}_\infty(\mathrm{SL}_2(\mathbb{F}_q))| = q(q-1)$$

and hence

$$|\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))| = \frac{q(q-1)}{2}.$$

Notice that the only possible divisor of both $q(q-1)/2$ and $q+1$ is 2. But since $q \equiv 3 \mod 4$, $q(q-1)/2$ is odd and therefore

$$gcd(|\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))|, |D_{q+1}|) = 1.$$

We conclude that

$$\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q)) \cap D_{q+1} = \{id\}.$$

Therefore, since $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$ and D_{q+1} have complementary indices, one can choose all coset representatives for D_{q+1} in $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$.

Recall that we have chosen $\mathcal{P}$ to be a prime such that $\mathcal{O}_K^\times$ surjects $\mathbb{F}_q^\times$. It follows that for all

$$\pm\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$$

there is an $\alpha \in \mathcal{O}_K^\times$ and $\beta \in \mathcal{O}_K$ such that

$$\phi_{\mathcal{P}}\left(\pm\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}\right) = \pm\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

As $\Gamma(\mathcal{P}) < \Gamma$ we have $q(q-1)/2$ distinct coset representatives for Γ in $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K))$. Therefore, we have a coset decomposition for $\mathrm{PSL}_2(\mathcal{O}_K)$ with representatives

$$\pm\begin{pmatrix} f^y & x_i \\ 0 & f^{-y} \end{pmatrix}\Gamma$$

where $f \in \mathcal{O}_K^\times$ maps onto a generator of $(\mathcal{O}_K/\mathcal{P})^\times$,

$$0 \leq y < \frac{1}{2}|(\mathcal{O}_K/\mathcal{P})^\times| = (q-1)/2$$

and for $0 \leq i < N(\mathcal{P})$, the x_i are unique representatives for $\mathcal{O}_K/\mathcal{P}$. We conclude that Γ has one cusp.

Proof. (Proof of Lemma 2.0.1)

We will be making a straightforward application of [12] Theorem 3.1. Following [12], let K be a number field, $\mathcal{P}$ a non-zero prime ideal of K, F a Galois extension of K, $C \subset Gal(F/K)$ a union of conjugacy classes, and $W \subset \mathcal{O}_K^\times$ a subset of positive rank modulo its torsion subgroup. Recall that the Frobenius Symbol $(\mathcal{P}, F/K)$ denotes the set of $\sigma \in Gal(F/K)$ for which there is a prime $\mathcal{Q}$ in F lying over $\mathcal{P}$ such that $\sigma(\mathcal{Q}) = \mathcal{Q}$ and $\sigma(\alpha) \equiv \alpha^{N(\mathcal{P})}$ mod $\mathcal{Q}$. Let the set $M(K, F, C, W, k)$ denote those primes $\mathcal{P}$ of K which satisfy $(\mathcal{P}, F/K) \subset C$, $ord_{\mathcal{P}}(w) = 0$ for all $w \in W$, and such that $\phi : W \to (\mathcal{O}_K/\mathcal{P})^\times$ has index divisible by k. Let μ be the Mobius function,

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has one or more repeated roots} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \end{cases}$$

ζ_n, a primitive n^{th} root of unity,

$$L_n = K(\zeta_n, (\mathcal{O}_K^\times)^{1/n}),$$

and

$$c(n) = |\{\sigma\} \cap Gal(K(i)/(K(i) \cap L_n)|.$$

Define

$$d(M) = \sum_n \frac{\mu(n)c(n)}{[F \cdot L_n : K]}.$$

Assuming the GRH, it is shown that $M(K, F, C, W, k)$ has a natural density equal to $d(M)$.

Now we will apply this to our situation. Let K be a number field other than $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$, with the added condition that K does not contain i. Therefore $K(i)$ is a degree 2 extension of K and $Gal(K(i)/K) = \{\sigma, id\}$ where σ is complex conjugation. Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$. By [12], for $M = M(K, K(i), \{\sigma\}, \mathcal{O}_K^\times, 1)$,

$$d(M) = \sum_n \frac{\mu(n)c(n)}{[K(i) \cdot L_n : K]}.$$

We see that $[K(i) \cdot L_n : K] = 2[L_n : K]$, and

$$c(n) = \begin{cases} 1 & \text{if } 4 \not| n \\ 0 & \text{if } 4|n. \end{cases}$$

But as $\mu(n) = 0$ if $4|n$

$$d(M) = \frac{1}{2} \sum_n \frac{\mu(n)}{[L_n : K]}$$

and therefore

$$d(M) = 2d(M(K, K, \{id\}, \mathcal{O}_K^\times, 1))$$

which is seen to be non-zero by the criteria in [12].

The condition that $k = 1$ corresponds to the map $\mathcal{O}_K^\times \to (\mathcal{O}/\mathcal{P})^\times$ being surjective. So it suffices to see that the unramified primes in

$$M(K, K(i), \{\sigma\}, \mathcal{O}_K^\times, 1)$$

are precisely those unramified primes $\mathcal{P}$ in K such that $N(\mathcal{P}) \equiv 3 \mod 4$. Assume that $\mathcal{P}$ is unramified. First, notice that a prime in the extension $K(i)/K$ splits precisely when $N(\mathcal{P}) \equiv 1 \mod 4$. This is because in $K(i)$ a prime ideal of K always splits as $\mathcal{P} = (n+i)(n-i)$ and so $n^2 \equiv -1 \mod \mathcal{P}$. The group $(\mathcal{O}_K/\mathcal{P})^\times \cong \mathbb{Z}_{q-1}$ and -1 corresponds to $(q-1)/2$. Therefore $-1 \equiv n^2$ for some n if and only if $(q-1)/2$ is even, that is precisely when $q \equiv 1 \mod 4$. Moreover, when there is an n with $n^2 \equiv -1$ we obtain a split. It is now enough to see that $(\mathcal{P}, K(i)/K) \subset \{\sigma\}$ occurs precisely when $\mathcal{P}$ is inert in $K(i)$, and hence $N(\mathcal{P}) \equiv 3 \mod 4$. If σ is complex conjugation, the condition $\sigma(\mathcal{Q}) = \mathcal{Q}$ for $\mathcal{Q}$ lying over $\mathcal{P}$ occurs only when $\mathcal{P}$ is inert in $K(i)$, and here $\sigma(\alpha) \equiv \alpha^{N(\mathcal{P})}$.

□

Chapter 3

Key Lemmas

In this chapter we will state and prove several key lemmas used in the proof of Theorem 1.1.1. Recall that $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$ has $\mathcal{O}_K$-level L if L is the ideal in $\mathcal{O}_K$ maximal with the property that the normal closure of the group generated by

$$\left\{ \pm \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} : l \in L \right\}$$

is contained in Γ.

3.1 Wohlfahrt's Lemma

Theorem 3.1.1. *Let K be a number field with class number one, and let $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$ be a congruence subgroup of $\mathcal{O}_K$-level (n). Then $(r) \subseteq (n)$ if and only if Γ contains $\Gamma(r)$.*

Proof. The proof is a modification from the case where $K = \mathbb{Q}$ [7]. First, assume that $\Gamma(r) < \Gamma$. Since the $\mathcal{O}_K$-level of Γ is (n), (n) is maximal with respect to the property that the normal closure of the group generated by

$$\left\{ \pm \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} : \mu \in (n) \right\}$$

is in Γ. We will show that $(r) \subseteq (n)$. Notice that for any $x \in \mathcal{O}_K$, since both

$$\pm \begin{pmatrix} 1 & rx \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}$$

are elements of Γ, then

$$\pm \begin{pmatrix} 1 & gx \\ 0 & 1 \end{pmatrix} \in \Gamma$$

where $(g) = (r, n)$ as ideals. Since (n) is maximal with this property, we conclude that $(g) = (n)$ and so $(r) \subseteq (n)$.

Now it suffices to show that if the $\mathcal{O}_K$-level of Γ is (n) and $(r) \subseteq (n)$ then $\Gamma(r) < \Gamma$. It is enough to show that $\Gamma(n) < \Gamma$ as if $(r) \subseteq (n)$ then $\Gamma(r) < \Gamma(n)$. The proof will be a consequence of the following.

Lemma 3.1.2. *Let K be a number field with class number one and let $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$ be a congruence subgroup of $\mathcal{O}_K$-level (n). If $\Gamma(mn) < \Gamma$ then $\Gamma(n) < \Gamma$.*

Assuming this lemma, let Γ be a congruence subgroup with $\mathcal{O}_K$-level (n). Therefore, $\Gamma(l) < \Gamma$ for some non-zero $l \in \mathcal{O}_K$ and so

$$\pm \begin{pmatrix} 1 & lx \\ 0 & 1 \end{pmatrix} \in \Gamma$$

for all $x \in \mathcal{O}_K$. By the maximality of (n), we conclude that $(l) \subseteq (n)$. As a result, there is an $(m) \in \mathcal{O}_K$ such that $(l) = (mn)$ and by the lemma we see that $\Gamma(n) < \Gamma$.

Now we will prove the lemma. By hypothesis, Γ has level (n) so the normal closure of the group generated by

$$\left\{ \pm \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} : \mu \in (n) \right\}$$

is contained in Γ. Hence for all x, y, and $z \in \mathcal{O}_K$, the following elements are in Γ

$$S_n(x) = \pm \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}, W_n(y) = \pm \begin{pmatrix} 1 & 0 \\ ny & 1 \end{pmatrix},$$

$$\begin{aligned} V_n(z) &= \pm \begin{pmatrix} -1 & 0 \\ z & -1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ z & -1 \end{pmatrix} \\ &= \pm \begin{pmatrix} 1+nz & -n \\ nz^2 & 1-nz \end{pmatrix}. \end{aligned}$$

Notice that $S_{-n}(x) = S_n(x)^{-1}$ and $W_{-n}(y) = W_n(y)^{-1}$. Suppose that $T \in \Gamma(n)$. To prove the lemma it suffices to show that $T \in \Gamma$. T has the form

$$T = \pm \begin{pmatrix} 1+na & nb \\ nc & 1+nd \end{pmatrix}$$

for some a, b, c, and $d \in \mathcal{O}_K$. Since $\det T = 1$, we see that $(1+na, nc) = \mathcal{O}_K$ and so $(1+na, n^2c) = \mathcal{O}_K$. By Corollary 1.2.2, for m as in the statement of the lemma, there is an $x \in \mathcal{O}_K$ such that $((1+na) + (n^2c)x, m) = \mathcal{O}_K$.

Let $T_1 = S_n(x)T$ for x as above. To show $T \in \Gamma$ it suffices to show that $T_1 \in \Gamma$ as $S_n(x) \in \Gamma$.

$$T_1 = \pm \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+na & nb \\ nc & 1+nd \end{pmatrix}$$

$$= \pm \begin{pmatrix} 1+n(a+nxc) & n(b+x+ndx) \\ nc & 1+nd \end{pmatrix} = \pm \begin{pmatrix} 1+na_1 & nb_1 \\ nc & 1+nd \end{pmatrix}$$

with $a_1 = a + ncx$, $b_1 = b + x + ndx$. Therefore

$$(1+na_1, m) = ((1+na) + (n^2c)x, m) = \mathcal{O}_K.$$

Now, considering z as a variable, let $T_2 = V_n(z)T_1$. To show that $T_1 \in \Gamma$ it suffices to show that $T_2 \in \Gamma$.

$$T_2 = \pm \begin{pmatrix} 1+nz & -n \\ nz^2 & 1-nz \end{pmatrix} \begin{pmatrix} 1+na_1 & nb_1 \\ nc & 1+nd \end{pmatrix}$$

$$= \pm \begin{pmatrix} (1+nz)(1+na_1) - n^2c & n(b_1 + b_1nz - 1 - nd) \\ (1+na_1)nz^2 + (1-nz)nc & 1 + n(nz^2b_1 - z + d - ndz) \end{pmatrix}.$$

Fix attention on the (1,1) entry,

$$(1+nz)(1+na_1) - n^2c = 1 + n(a_1 + z + na_1z - nc).$$

Claim 3.1.3. *There is a $z \in \mathcal{O}_K$ such that $1 + n(a_1 + z + na_1z - nc) \equiv 1 \mod mn$.*

Proof. Note that this statement is equivalent to

$$(a_1 - nc) + z(1 + na_1) \equiv 0 \mod m.$$

But as above, $(1 + na_1, m) = \mathcal{O}_K$, and since $\mathcal{O}_K$ is a PID, there are $s, t \in \mathcal{O}_K$ such that $s(1 + na_1) + t(m) = 1$ and therefore $tm = 1 + (-s)(1 + na_1)$ and

$$[t(a_1 - nc)]m = (a_1 - nc) + [(-s)(1 + na_1)](1 + na_1).$$

Thus $z = (-s)(1 + na_1)$ is a solution. □

For some such solution z, we have

$$T_2 = \pm \begin{pmatrix} 1 & nb_2 \\ nc_2 & 1 + nd_2 \end{pmatrix} \mod mn$$

where $d_2 = nz^2b_1 - z + d - ndz$. As can be checked,

$$T_2 = \pm W_n(c_2)S_n(b_2) \mod mn$$

since $\det(T_2) = 1 \equiv 1 + nd_2 - n^2b_2c_2 \mod mn$. Therefore $d_2 \equiv nb_2c_2 \mod m$. We deduce

$$S_{-n}(b_2)W_{-n}(c_2)T_2 = \pm 1 \mod mn,$$

and since $\Gamma(mn) < \Gamma$, we have

$$S_{-n}(b_2)W_{-n}(c_2)T_2 \in \Gamma$$

hence

$$T_2 = V_n(z)T_1 \in \Gamma$$

and $T_1 = S_n(x)T \in \Gamma$ and so $T \in \Gamma$, completing the proof. □

Notice that the the principal congruence subgroup $\Gamma(n)$ contains $\Gamma(m)$ for all m such that $(m) \subset (n)$. Therefore, if K has class number one and if $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$ contains principal congruence subgroups $\Gamma(n_1)$ and $\Gamma(n_2)$, then $\Gamma(n) < \Gamma$ where $(n) = (n_1, n_2)$. As a result, there is an $(n) \subset \mathcal{O}_K$ that is maximal with respect to inclusion (of ideals) such that $\Gamma(n) < \Gamma$. By Wohlfahrt's Theorem, we know that this (n) is determined by $\Lambda(\Gamma)$, and is the $\mathcal{O}_K$-level of Γ. By the same reasoning, if Γ has $\mathbb{Z}$-level (n), then (n) is maximal with respect to inclusion over all principal ideals generated by an element in $\mathbb{Z}$ with the property that $\Gamma(n) < \Gamma$. We have

Corollary 3.1.4. *Let K be a number field with class number one, and let $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$ be a congruence subgroup.*

1. Γ has $\mathbb{Z}$-level (n) if and only if $\Gamma(n)$ is the maximal principal congruence subgroup contained in Γ whose level can be generated by a rational integer.

2. Γ has $\mathcal{O}_K$-level (n) if and only if $\Gamma(n)$ is the maximal principal congruence subgroup contained in Γ.

3. Let Γ have $\mathcal{O}_K$-level (m) and $\mathbb{Z}$-level (n). Then n is the smallest positive integer such that $(n) \subset (m)$.

3.2 The Ladder Lemma

In the following, let K be a PID. If $x \in \mathcal{O}_K$ and y is a non-zero element of $\mathcal{O}_K$ then (x/y) will denote the fractional ideal $(x)J$ where J is the fractional ideal that is the inverse of (y), $J(y) = \mathcal{O}_K$. If $(x) \subset (y)$ then (x/y) is an ideal.

Lemma 3.2.1. *Let K be a number field with class number one. Let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ of $\mathcal{O}_K$-level (m). Let $\mathcal{P}_1 \dots \mathcal{P}_n$ be primes in $\mathcal{O}_K$ lying over p a prime in $\mathbb{Z}$, and let $(d) = \mathcal{P}_1^{r_1}\mathcal{P}_2^{r_2}\dots\mathcal{P}_n^{r_n}$ such that $(m) \subset (d)$ and $1 \leq r_j \leq e_j$, the ramification index of $\mathcal{P}_j$ in $\mathcal{O}_K$. If s_j is the maximal power of $\mathcal{P}_j$ dividing (m), and*

$$s_j \geq \begin{cases} r_j + 2e_j & \text{if } \ p = 2 \\ e_j + \lceil \frac{r_j}{2} \rceil + 1 & \text{if } \ p = 3 \\ 2r_j & \text{for all } p \end{cases}$$

where $\lceil r \rceil$ is the ceiling function, then $\Gamma\Gamma(m/d)$ is a one-cusped congruence subgroup of $\mathcal{O}_K$-level at least $(m)/(m) \cap (a)$, where a is the smallest positive integer that (d) divides.

When K is an imaginary quadratic we have the following corollary, which we will use in the proof of Theorem 1.1.1.

Corollary 3.2.2. *Let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$. If Γ has $\mathbb{Z}$-level p^n where p is a prime and*

$$n \geq \begin{cases} 3 & p \leq 3 \\ 2 & p > 3 \end{cases}$$

then $\Gamma\Gamma(p^{n-1})$ has $\mathbb{Z}$-level p^{n-1}. If Γ has $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is ramified, then if

$$n \geq \begin{cases} 5 & p = 2 \\ 4 & p = 3 \\ 3 & p > 5 \end{cases}$$

then $\Gamma\Gamma(\mathcal{P}^{n-1})$ has $\mathcal{O}_d$-level $\mathcal{P}^{n-1}$ or $\mathcal{P}^{n-2}$.

Proof. (proof of lemma)

Let $\{\omega_1, \omega_2, \ldots \omega_k\}$ be an integral basis for K. First, we will prove the lemma for $p > 3$. Let Γ be as in the statement of the lemma and let $(\mu) = (m/d)$. Consider an element $X \in \Gamma\Gamma(\mu)$ of the form

$$X = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Then $X = AB$ where $A \in \Gamma$ and $B \in \Gamma(\mu)$, and so there is a $M \in M_2(\mathcal{O}_K)$ such that $A = X + \mu M$. Since $(d) = \mathcal{P}_1^{r_1} \ldots \mathcal{P}_n^{r_n}$ and $\mathcal{P}_1^{s_1} \ldots \mathcal{P}_n^{s_n}$ divides (m) with $s_j \geq 2r_j$, (m) divides (μ^2), implying that

$$A^p = [X + \mu M]^p \equiv X^p + \mu W X^{(p-1)} \mod (m)$$

with

$$W = \sum_{j=0}^{p-1} X^j M X^{-j} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \mod (p).$$

So $A^p \equiv X^p \mod (m)$ and there is a $C \in \Gamma(m)$ such that $X^p = A^p C$. We conclude that for $1 \leq i \leq k$,

$$X^p = \begin{pmatrix} 1 & px \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

If (l) is the $\mathcal{O}_K$-level of $\Gamma\Gamma(\mu)$, choosing $x = l\omega_i$ we see that for $1 \leq i \leq k$

$$\begin{pmatrix} 1 & l\omega_i \\ 0 & 1 \end{pmatrix} \in \Gamma\Gamma(\mu),$$

and therefore

$$\begin{pmatrix} 1 & pl\omega_i \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

So (m) divides (pl), and by Wohlfahrt's theorem, the $\mathcal{O}_K$-level of $\Gamma\Gamma(\mu)$ is at least $(m)/(m) \cap (a)$ where (a) is as in the statement of the lemma.

Now consider the case where $p = 2$. As before, we have $A = X + \mu M$. Therefore

$$A^4 = [X + \mu M]^4 = X^4 + \mu W_1 X^3 + \mu^2 Y$$

where $Y \in M_2(\mathcal{O}_K)$ and

$$W_1 = \sum_{j=0}^{3} X^j M X^{-j} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \mod (2).$$

As (d) divides (2), $\mu W_1 X^3 \equiv 0 \mod (m)$ and since (m) divides (μ^2),

$$A^4 \equiv X^4 \mod (m).$$

Therefore $X^4 \in \Gamma$. Setting $x = \omega_i l$ where (l) is the $\mathcal{O}_K$-level of $\Gamma\Gamma(\mu)$, then we conclude that for $1 \leq i \leq k$,

$$\begin{pmatrix} 1 & 4\omega_i l \\ 0 & 1 \end{pmatrix} \in \Gamma$$

and so (m) divides $(4l)$. We conclude that (d) divides (l), as $s_j > r_j + 2e_j$.

Now consider

$$A^2 = [X + \mu M]^2 = X^2 + \mu XM + \mu MX + \mu^2 M^2$$

$$= X^2 + \mu[M + XMX^{-1}]X + \mu^2 M^2.$$

Letting $W = M + XMX^{-1}$, $W \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \mod (d)$ if (x) is divisible by (d). We conclude that if (d) divides (x), $A^2 \equiv X^2 \mod (m)$. Setting $x = \omega_i l$, by above, (d) divides (l) and so $A^2 \equiv X^2 \mod (m)$ and therefore $X^2 \in \Gamma$. So for $i \leq i \leq k$,

$$\begin{pmatrix} 1 & 2l\omega_i \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

Implying that (m) divides $(2l)$ by Wohlfahrt's theorem, finishing the proof in this case.

Finally, let $p = 3$. As before, we have $A = X + \mu M$, and so

$$A^3 = [X + \mu M]^3 = X^3 + \mu W X^2 + \mu^2 Y$$

for $Y \in M_2(\mathcal{O}_K)$ and

$$W = \sum_{j=0}^{2} X^j M X^{-j} \equiv \begin{pmatrix} 0 & x^2 m_2 \\ 0 & 0 \end{pmatrix} \mod 3.$$

So, $A^3 \equiv X^3 + \mu \begin{pmatrix} 0 & x^2 m_2 \\ 0 & 0 \end{pmatrix} X^2 \mod (m)$ and

$$X^3 + \mu \begin{pmatrix} 0 & x^2 m_2 \\ 0 & 0 \end{pmatrix} X^2 = \begin{pmatrix} 1 & 3x + \mu x^2 m_2 \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

Letting $x = \omega_i l$ we see that

$$\begin{pmatrix} 1 & 3l\omega_i + \mu l^2 m_2 \omega_i^2 \\ 0 & 1 \end{pmatrix} \in \Gamma$$

for $1 \leq i \leq k$. If (d) divides (l^2), then

$$\begin{pmatrix} 1 & 3l\omega_i \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

And so the $\mathcal{O}_K$-level of $\Gamma\Gamma(\mu)$ is at least $(m)/(m) \cap (a)$ where (a) is as above. If (d) does not divide (l^2) then $(l) = \mathcal{P}_1^{t_1} \dots \mathcal{P}_n^{t_m} Z$ where $t_j \geq 0$ for $1 \leq j \leq n$ and Z is relatively prime to $\mathcal{P}_1 \cdots \mathcal{P}_n$. Moreover, there is a k with $1 \leq k \leq n$, such that $2t_k \leq r_k$. Let $y = \mathcal{P}_1^{m_1} \cdots \mathcal{P}_n^{m_n} Z$ where $m_j = \max\{t_j, \lceil r_j/2 \rceil\}$. Therefore (l) divides (y) and $y \in \Lambda(\Gamma\Gamma(\mu))$. Since $r_j \geq 2\max\{t_j, \lceil r_j/2 \rceil\}$ we conclude that (d) divides (y^2) and setting $x = y\omega_i$ we have

$$\begin{pmatrix} 1 & 3y\omega_i \\ 0 & 1 \end{pmatrix} \in \Gamma$$

for $1 \leq i \leq k$. As a result, for $1 \leq j \leq n$, $e_j + \max\{t_j + \lceil r_j/2 \rceil\} \leq s_j$. But, $\max\{t_k, \lceil r_k/2 \rceil\} = \lceil r_k/2 \rceil$ and therefore $e_k + \lceil r_k/2 \rceil \geq s_k$ which contradicts our initial assumption.

□

3.3 The Index Lemma

Lemma 3.3.1. *Let K be a number field with class number one and let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ of $\mathbb{Z}$-level $p^t m$ where p is a prime and $(m, p) = 1$. If $p > 3$ then p^t divides $[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]$. If $p \leq 3$, then p^s divides $[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]$ where $s = t$ if p divides the $\mathbb{Z}$-level of $\Gamma\Gamma(pm)$ and $s = t - 1$ otherwise.*

Proof. If $\Gamma < \mathrm{PSL}_2(\mathcal{O}_K)$, recall that

$$\Lambda(\Gamma) = \left\{ c \in \mathcal{O}_k : \pm \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in \Gamma \right\}.$$

Let $k = [K : \mathbb{Q}]$, and fix an integral basis $\{\omega_1, \ldots, \omega_k\}$ for $\mathcal{O}_K$. Define

$$\psi : \Lambda(\mathrm{PSL}_2(\mathcal{O}_K)) \to \mathbb{Z}^k$$

by defining

$$\psi(\omega_i) = (0, \ldots, 1, \ldots 0)$$

where the 1 is in the i^{th} position and extending. Let A be the subgroup of $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K))$ consisting of elements of the form

$$\begin{pmatrix} f & x \\ 0 & f^{-1} \end{pmatrix}$$

where f is a unit in $\mathcal{O}_K$ other than ± 1, and let $T = [A : A \cap \Gamma]$. Notice that

$$\frac{|\Lambda(\mathrm{PSL}_2(\mathcal{O}_K))|}{|\Lambda(\Gamma)|} = [\psi(\Lambda(\mathrm{PSL}_2(\mathcal{O}_K))) : \psi(\Lambda(\Gamma))].$$

By Lemma 1.4.1, if Γ has one cusp, then

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\infty(\Gamma)]$$

and therefore

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [\psi(\Lambda(\mathrm{PSL}_2(\mathcal{O}_K))) : \psi(\Lambda(\Gamma))]T.$$

Let $G = \psi(\Lambda(PSL_2(\mathcal{O}_K)))$, $G_\Gamma = \psi(\Lambda(\Gamma))$, and $G_n = \psi(\Lambda(\Gamma(n)))$ for any non-zero $n \in \mathcal{O}_K$. So

$$[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma] = [G : G_\Gamma]T.$$

We will show that if $p > 3$ or if $p \leq 3$ and p divides the $\mathbb{Z}$-level of $\Gamma\Gamma(pm)$, then p^t divides $[G : G_\Gamma]$. If $p = 2$ or 3 and p does not divide the $\mathbb{Z}$-level $\Gamma\Gamma(pm)$, we will show that p^{t-1} divides $[G : G_\Gamma]$.

Notice that $\Lambda(\mathrm{PSL}_2(\mathcal{O}_K))$ is generated by the elements $\{\omega_1, \omega_2, \ldots \omega_k\}$, and $\Lambda(\Gamma(n))$ is generated by $\{n\omega_1, n\omega_2, \ldots n\omega_k\}$. Therefore G is generated by the elements $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0), \ldots (0, 0, \ldots, 1)$ and G_n is generated by the elements $(n, 0, \ldots, 0)$, $(0, n, \ldots, 0), \ldots (0, 0, \ldots, n)$. As a result, $[G : G_n] = n^k$, and similarly, if m divides n, $[G_m : G_n] = (m/n)^k$.

Fix m and p. First consider the case where $t = 1$. We will induct on t. Assume that p does not divide $[G : G_\Gamma]$. Therefore p does not divide $[G_\Gamma G_m : G_\Gamma]$ or $[G : G_\Gamma G_m]$. But, p^k divides $[G : G_{pm}]$ and so p^k divides $[G_\Gamma : G_{pm}]$. Since $[G_m : G_{pm}] = p^k$ and p does not divide $[G_m : G_\Gamma \cap G_m]$

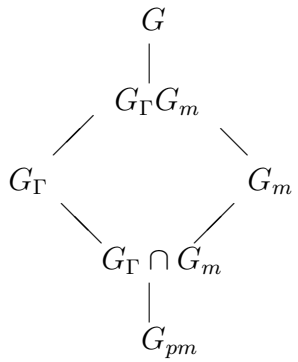

Figure 3.1: The case $t = 1$

(which equals $[G_\Gamma G_m : G_\Gamma]$ by the second isomorphism theorem) we conclude that

$$[G_\Gamma \cap G_m : G_{pm}] = p^k$$

and so $G_m = G_\Gamma \cap G_m$, and thus $G_m < G_\Gamma$. This implies that

$$\pm \begin{pmatrix} 1 & m\omega_i \\ 0 & 1 \end{pmatrix} \in \Gamma$$

for $1 \leq i \leq k$. By Wohlfahrt's theorem, the $\mathbb{Z}$-level of Γ divides m contradicting the hypothesis that it is pm.

In the case where $p = 2$ or 3, if $t = 2$ and p does not divide the $\mathbb{Z}$-level of $\Gamma\Gamma(pm)$ we use a similar argument to conclude that p divides $[G : G_\Gamma]$. This proves the second case for $t \leq 3$.

Now assume that for all s such that $1 < s < t$, that for all one-cusped Γ of $\mathbb{Z}$-level $p^s m$, p^s divides $[G : G_\Gamma]$. First, consider the case where $p > 3$ or $p \leq 3$ and the $\mathbb{Z}$-level of $\Gamma\Gamma(pm)$ is pm. Assume that Γ is a one-cusped

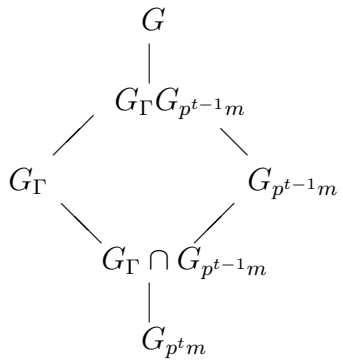

Figure 3.2: The General Case

congruence subgroup of $\mathbb{Z}$-level $p^t m$ and p^t does not divide $[G : G_\Gamma]$. Notice that $G_\Gamma G_{p^{t-1}m} = G_{\Gamma\Gamma(p^{t-1}m)}$ and so by the Ladder Lemma and the inductive hypothesis, p^{t-1} divides $[G : G_\Gamma G_{p^{t-1}m}]$. So p does not divide

$$[G_\Gamma G_{p^{t-1}m} : G_\Gamma] = [G_{p^{t-1}m} : G_\Gamma \cap G_{p^{t-1}m}],$$

but $[G_{p^{t-1}m} : G_{p^t m}] = p^k$ and so $G_{p^{t-1}m} = G_\Gamma \cap G_{p^{t-1}m}$ implying that $G_{p^{t-1}m} < G_\Gamma$. This implies that

$$\pm \begin{pmatrix} 1 & p^{t-1}m\omega_i \\ 1 & 1 \end{pmatrix} \in \Gamma$$

for $1 \leq i \leq k$. This contradicts Wohlfahrt's theorem as the $\mathbb{Z}$-level of Γ is $p^t m$. We conclude that p^t divides $[G : G_\Gamma]$ and so p^t divides $[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]$.

If $p = 2$ or 3 and $t \geq 3$, if p^2 divides $[G : G_\Gamma G_{p^2 m}]$ we also conclude that p^t divides $[G : G_\Gamma]$. Otherwise, we have seen that p divides $[G : G_\Gamma G_{p^2 m}]$ and similar to above we conclude that p^{t-1} divides $[G : G_\Gamma]$ and therefore p^{t-1} divides $[\mathrm{PSL}_2(\mathcal{O}_K) : \Gamma]$.

□

3.4 The Peripheral Lattice

In this section we will analyze the possible peripheral lattices that can occur for certain $\mathcal{O}_d$-levels of subgroups of $\mathrm{PSL}_2(\mathcal{O}_d)$. Recall that if $\Gamma < \mathrm{PSL}_2(\mathcal{O}_d)$

$$\Lambda(\Gamma) = \left\{ c \in \mathcal{O}_d : \pm \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in \Gamma \right\}.$$

Let $\{1, \omega\}$ be a fixed integral basis for $\mathcal{O}_d$. By Wohlfahrt's theorem, if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level (n) then $\Lambda(\Gamma)$ contains n and ωn, but not both m and ωm for any $(m) \not\subset (n)$. The following definitions will be useful in this discussion.

Definition 3.4.1. For $\Gamma < \mathrm{PSL}_2(\mathcal{O}_d)$, given a non-zero $x \in \mathcal{O}_d$ we define $\Lambda_x(\Gamma)$ to be the minimal positive integer n such that $nx \in \Lambda(\Gamma)$. Let $\Gamma < \mathrm{PSL}_2(\mathcal{O}_d)$ be a congruence subgroup of $\mathbb{Z}$-level n. Then $\mathcal{D}$ is a *proper diagonal* of $\Lambda(\Gamma)$ if $\mathcal{D}$ is a primitive element of $\Lambda(\Gamma)$ such that $\mathcal{D} = a + b\omega$ for $0 \leq a, b < n$.

Let Γ be a one-cusped congruence subgroup of $\mathbb{Z}$-level p^n for a prime p. By Wohlfahrt's Theorem either $\Lambda_1(\Gamma)$ or $\Lambda_\omega(\Gamma)$ equals p^n and the other is p^k for some k such that $0 \leq k \leq n$ as otherwise a smaller lattice is contained in $\Lambda(\Gamma)$. Assume that $\Lambda_1(\Gamma) = p^n$ and $\Lambda_\omega(\Gamma) = p^k$ for $0 \leq k \leq n$. (The case where $\Lambda_1(\Gamma) \leq \Lambda_\omega(\Gamma)$ is completely analogous.) We will show that all elements of $\Lambda(\Gamma)$ are of the form

$$A\mathcal{D}(\Gamma) + B\Lambda_1(\Gamma) + C\Lambda_\omega(\Gamma)$$

where $\mathcal{D}(\Gamma)$ is of the form $p^r(gp^{n-k} + g'\omega)$ with $0 < r < k$ and non-zero, g and g' relatively prime to p, and A, B, and $C \in \mathbb{Z}$. Let $a \in \Lambda(\Gamma)$.

It suffices to consider elements of the form

$$a = p^r(gp^t + g'\omega).$$

If $t < n - k$ then $p^{k-r}a = p^{k+t}g + g'p^k\omega \in \Lambda(\Gamma)$ and therefore $p^{k+t}g \in \Lambda(\Gamma)$. Since $(p, g) = 1$, $p^{k+t} \in \Lambda(\Gamma)$, but this cannot occur as $k + t < n$. If $t > n - k$ then $p^{n-(t+r)}a = p^n g + p^{n-t}g'\omega \in \Lambda(\Gamma)$ and so $p^{n-t}\omega \in \Lambda(\Gamma)$, which cannot occur as $n - t < k$. If

$$a = p^r(g + p^t g'\omega)$$

and $r + t \geq k$ we have an immediate contradiction, and if $r + t < k$, the fact that $p^{k-(r+t)}a = p^{k-t}g + p^k g'\omega \in \Lambda(\Gamma)$ implies that $p^{k-t} \in \Lambda(\Gamma)$. Therefore all elements of $\Lambda(\Gamma)$ are of the above form.

Now, let $\mathcal{D}$ be the diagonal element with minimal exponent r with respect to the above notation. So

$$A\mathcal{D} = Ap^r(gp^{n-k} + \omega g').$$

Since g, g', and A are relatively prime to p, there are $c_1, c_2 \in \mathbb{Z}$ such that $c_1 Ag + c_2 p^{k-r} = 1$. Therefore $c_1 A\mathcal{D} = p^{r+n-k} - c_2 p^n + c_1 Ag' p^r \omega \in \Lambda(\Gamma)$. So $p^r(p^{n-k} + h'\omega) \in \Lambda(\Gamma)$ for $h' \in \mathbb{Z}$, $(h', p) = 1$ and $0 < h' < p^n$. We have diagonals $\mathcal{D}_1 = p^r(p^{n-k} + \omega h')$ and $\mathcal{D}_2 = p^r(hp^{n-k} + \omega)$ where both h and h' are relatively prime to p. Now, we will appeal to a theorem in the geometry of numbers [9], which states

Theorem 3.4.1. *(Theorem on Lattice Triangles) Let b^1, b^2 be two independent points of a lattice Λ in $\mathbb{R}^2$. Suppose that the closed triangle with vertices 0, b^1, b^2 does not contain other points of Λ. Then $\{b^1, b^2\}$ is a basis of Λ.*

So, $\{\mathcal{D}_1, \Lambda_1(\Gamma)\}$, and $\{\mathcal{D}_2, \Lambda_\omega(\Gamma)\}$ are both bases for $\Lambda(\Gamma)$, whose normalized area is p^{n+r}. And we have shown

Proposition 3.4.2. *Let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ of $\mathbb{Z}$-level p^n where p is a prime. Then $\Lambda(\Gamma)$ is generated by $\{\Lambda_1(\Gamma), \Lambda_\omega(\Gamma)\}$ if there are no proper diagonals, and both $\{\Lambda_1(\Gamma), \mathcal{D}\}$ and $\{\mathcal{D}', \Lambda_\omega(\Gamma)\}$ are generating sets for appropriate diagonals $\mathcal{D}$ and $\mathcal{D}'$ in $\Lambda(\Gamma)$.*

Notice that if $\mathcal{D} = p^r(gp^{n-k} + \omega)$ then all other elements of the form $p^r(hp^{n-k} + \omega h')$ are multiples of $\mathcal{D}$ modulo p^n and ωp^k, i.e. there are α, β, and $\gamma \in \mathbb{Z}$ such that $p^r(hp^{n-k} + \omega h') = \alpha\mathcal{D} + \beta p^n + \gamma\omega p^k$.

3.5 The Structure of $\mathrm{SL}_2(\mathcal{O}_d)$

We will use the following to understand the index of related congruence subgroups:

Claim 3.5.1. *Let G be a finite group such that $G = G_1 \times G_2$, and let $B < G$. Let $\rho_i : G \to G_i$ be projection for $i = 1, 2$. Define $B_i = \rho_i(B)$ for $i = 1, 2$ and let $N_1 < G_1$ be defined as $N_1 = \{t_1 \in B_1 : (t_1, 1) \in B\}$ and $N_2 < G_2$ be defined as $N_2 = \{t_2 \in B_2 : (1, t_2) \in B\}$. Then*

$$\begin{aligned} &B_1/N_1 \cong B_2/N_2 \\ &|B| = |B_1||N_2| = |B_2||N_1| \\ &[G : B] = [G_1 : B_1][G_2 : N_2]. \end{aligned}$$

Proof. First, we will show that $N_1 \triangleleft B_1$. Let $n_1 \in N_1$ and $b_1 \in B_1$. By the definition of N_1, $(n_1, 1) \in B$ and since $b_1 \in B_1$ there is a $b_2 \in B_2$ such that $(b_1, b_2) \in B$. Therefore

$$(b_1, b_2)^{-1}(n_1, 1)(b_1, b_2) = (b_1^{-1} n_1 b_1, 1) \in B$$

which implies that $b_1^{-1} n_1 b_1 \in N_1$, showing that $N_1 \triangleleft B_1$. Similarly, $N_2 \triangleleft B_2$.

Now we will define an isomorphism $\psi : B_1/N_1 \to B_2/N_2$. Given $b_1 \in B_1$ we let $\psi(b_1 N_1) = b_2 N_2$ for any b_2 such that $(b_1, b_2) \in B$. First, notice that if (b_1, b_2) and $(b_1, \beta_2) \in B$ then $(1, \beta_2^{-1} b_2) \in B$ so $\beta_2^{-1} b_2 \in N_2$ and we conclude that $\beta_2 N_2 = b_2 N_2$. If $b_1, \beta_1 \in B$ and $b_1 N_1 = \beta_1 N_1$ then $\beta_1^{-1} b_1 \in N_1$, therefore $(\beta_1^{-1} b_1, 1) \in B$. Since $\beta_1 \in B_1$, there is a $b_2 \in B_2$ such that $(\beta_1, b_2) \in B$. Therefore

$$(\beta_1, b_2)(\beta_1^{-1} b_1, 1) = (b_1, b_2) \in B$$

and we see that $\psi(b_1 N_1) = \psi(\beta_1 N_1) = b_2 N_2$, and conclude that ψ is well defined.

To see that ψ is injective, notice that if $\psi(b_1 N_1) = \psi(\beta_1 N_1) = b_2 N_2$ then (b_1, b_2) and (β_1, b_2) are in B. Therefore

$$(b_1, b_2)^{-1}(\beta_1, b_2) = (b_1^{-1}\beta_1, 1) \in B$$

and $b_1^{-1}\beta_1 \in N_1$, implying that $b_1 N_1 = \beta_1 N_1$. For all $b_2 \in B_2$ there is a $b_1 \in B_1$ such that $(b_1, b_2) \in B$ and therefore $\psi(b_1 N_1) = b_2 N_2$, showing surjectivity.

Now it suffices to show that $|B| = |B_1||N_2|$. For $b_1 \in B_1$, let

$$n(b_1) = |\{b_2 \in B_2 : (b_1, b_2) \in B\}|.$$

We will show that $n(b_1) = |N_2|$. Let $b_1 \in B_1$, so there is a $b_2 \in B_2$ such that $(b_1, b_2) \in B$. For each $n_2 \in N_2$, $(1, n_2) \in B$, so $(b_1, b_2 n_2) \in B$ and we conclude that $n(b_1) \geq |N_2|$. Conversely, if both (b_1, b_2) and $(b_1, \beta_2) \in B$, then $(1, b_2 \beta_2^{-1}) \in B$ and so $b_2 \beta_2^{-1} \in N_2$ and we see that $|N_2| = n(b_1)$.

□

It will be necessary to work both in $\mathrm{PSL}_2(\mathcal{O}_d)$ and $\mathrm{SL}_2(\mathcal{O}_d)$. If Γ is a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ containing $\Gamma(n)$, then the pull back of Γ under the projectivization map $\mathrm{SL}_2(\mathcal{O}_d) \to \mathrm{PSL}_2(\mathcal{O}_d)$ is a group of the same index that we will refer to as Γ', which contains a principal congruence subgroup $\Gamma(n)'$ in $\mathrm{SL}_2(\mathcal{O}_d)$, where

$$\Gamma(n)' = \{M \in \mathrm{SL}_2(\mathcal{O}_d) : M \equiv \pm I \mod (n)\}.$$

A group denoted G' will always refer to the $\mathrm{SL}_2(R)$ pull-back of a group $G < \mathrm{PSL}_2(R)$, where $R = \mathcal{O}_d$ or a quotient of $\mathcal{O}_d$, and will never refer to the derived subgroup. Let $n = n_1 n_2$ such that $n_i \in \mathcal{O}_d$, $(n_1, n_2) = 1$ and $(n_1) \cap (n_2) = (n)$. Let

$$\phi'_n : \mathrm{SL}_2(\mathcal{O}_d) \to \mathrm{SL}_2(\mathcal{O}_d/(n))$$

and

$$\phi_n : \mathrm{PSL}_2(\mathcal{O}_d) \to \mathrm{PSL}_2(\mathcal{O}_d/(n))$$

be the modulo (n) maps. Notice that

$$\mathrm{SL}_2(\mathcal{O}_d)/\Gamma(n)' \cong \mathrm{SL}_2(\mathcal{O}_d/(n)),$$

$$\mathrm{PSL}_2(\mathcal{O}_d)/\Gamma(n) \cong \mathrm{PSL}_2(\mathcal{O}_d/(n))$$

and

$$\mathrm{SL}_2(\mathcal{O}_d)/\Gamma(n_1 n_2)' \cong \mathrm{SL}_2(\mathcal{O}_d/(n_1)) \times \mathrm{SL}_2(\mathcal{O}_d/(n_2)).[17]$$

We will use these isomorphic groups interchangeably. We will denote projection in the i^{th} coordinate as

$$\rho'_i : \mathrm{SL}_2(\mathcal{O}_d/(n)) \to \mathrm{SL}_2(\mathcal{O}_d/(n_i))$$

and

$$\rho_i : \mathrm{PSL}_2(\mathcal{O}_d/(n)) \to \mathrm{PSL}_2(\mathcal{O}_d/(n_i)).$$

Define

$$B' = \phi'_n(\Gamma'), B'_i = \rho'_i(B')$$

$$B = \phi_n(\Gamma), B_i = \rho_i(B).$$

N'_i will be defined with respect to B'_i, as above, and let $N_i = PN'_i$, the image of N'_i under the projectivization map. Notice that

$$B_i = \phi_{n_i}(\Gamma) = \phi_{n_i}(\Gamma\Gamma(n_i)),$$

as $\Gamma(n_i) = \ker\phi_{n_i}$, and the analogous statement is true for B'_i. Let

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = [\mathrm{SL}_2(\mathcal{O}_d) : \Gamma'].$$

Notice that since $\Gamma(n) < \Gamma$,

$$x = [\mathrm{PSL}_2(\mathcal{O}_d/(n)) : B] = [\mathrm{SL}_2(\mathcal{O}_d/(n)) : B'].$$

Let

$$x_i = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(n_i)] = [\mathrm{PSL}_2(\mathcal{O}_d/(n_i)) : B_i] = [\mathrm{SL}_2(\mathcal{O}_d)/(n_i)) : B'_i].$$

We define

$$M(n) = N(n)^3 \left[\prod_{\mathcal{P}|n} \left(1 - \frac{1}{N(\mathcal{P})^2}\right)\right] = |\mathrm{SL}_2(\mathcal{O}_d/(n))|$$

where the the product is taken over all primes $\mathcal{P}$ in $\mathcal{O}_d$ dividing (n). Notice that $M(n) = M(n_1)M(n_2)$ since $(n_1, n_2) = \mathcal{O}_d$. Therefore by the above algebraic statement

$$|N'_1| = \frac{|B'|}{|B'_2|} = \frac{x_2 M(n_1)}{x}, \text{and} |N'_2| = \frac{x_1 M(n_2)}{x}.$$

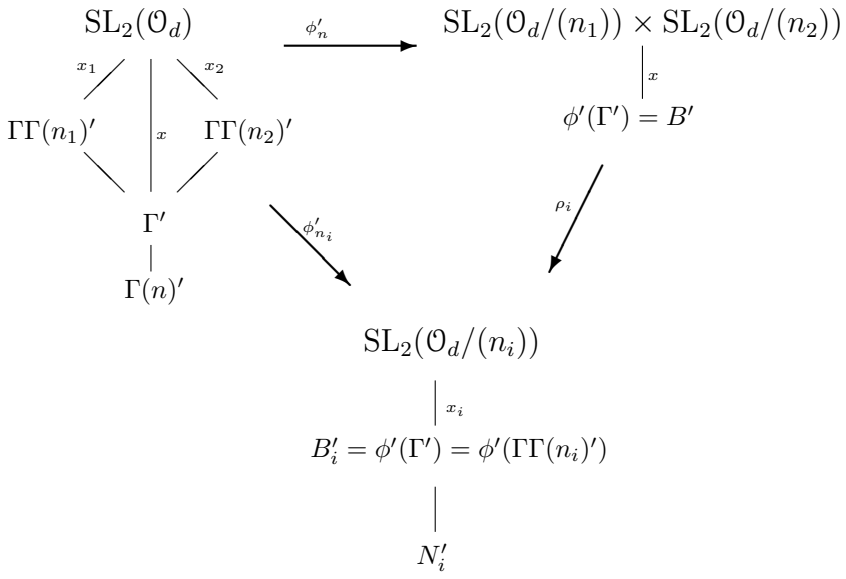

Figure 3.3: Commutative Diagram

Also,

$$[\mathrm{SL}_2(\mathcal{O}_d/(n_1)) : N'_1] = x/x_2$$

and

$$[\mathrm{SL}_2(\mathcal{O}_d/(n_2)) : N'_1] = x/x_1.$$

Therefore

$$[B'_1 : N'_1 = [B'_2 : N'_2] = \frac{x}{x_1 x_2}.$$

Notice that $|N_i| = \frac{1}{2}|N'_i|$ or $|N'_i|$, depending on whether $\pm I \in N'_i$ or not. (N'_i is defined with respect to B'_i, not as the pull-back of N_i.) If 2 does not divide $|\mathcal{O}_d/(n_i)|$

$$|N_1| = (2\mathrm{or}1)\frac{x_2}{x}M(n_1), \mathrm{and} |N_2| = (2\mathrm{or}1)\frac{x_1}{x}M(n_2).$$

If 2 divides $|\mathcal{O}_d/(n_i)|$, then $\mathcal{O}_d/(n_i) \cong \mathbb{F}_2$ or $\mathbb{F}_4$, $\mathrm{SL}_2(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_2)$ and $\mathrm{SL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_4)$ so $N_i' = N_i$, $B_i' = B_i$ and $B' = B$.

3.6 Vector Spaces

In this section we will describe a technique that will be used to encode information about one-cusped congruence subgroups, and especially their $\mathcal{O}_d$-levels, in terms of a vector subspace. This will be used as a convenient way to show that there cannot be one-cusped congruence subgroups in certain situations.

Let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is a prime lying over the rational prime p, $q \in \mathcal{O}_d$ is such that $(q) = \mathcal{P}$ and $n \geq 2$. If $p \neq 2$ the quotient $\Gamma(\mathcal{P}^{n-1})/\Gamma(\mathcal{P}^n)$ is a three-dimensional vector space, V, over $\mathbb{F}_{N(\mathcal{P})}$. For all p, the quotient $\Gamma(\mathcal{P}^{n-1})'/\Gamma(\mathcal{P}^n)'$ is a three-dimensional vector space over $\mathbb{F}_{N(\mathcal{P})}$. (When $p = 2$ the dimension of $\Gamma(\mathcal{P}^{n-1})/\Gamma(\mathcal{P}^n)$ varies for small powers of $\mathcal{P}$ corresponding to those cases when $\pm I \in \Gamma(\mathcal{P}^n)$.) The correspondence is given by

$$\pm \begin{pmatrix} 1 + q^{n-1}a & q^{n-1}b \\ q^{n-1}c & 1 + q^{n-1}d \end{pmatrix} \in \Gamma(\mathcal{P}^{n-1}) \leftrightarrow (a, b, c) \in V$$

for a, b, c, and d in $\mathcal{O}_d$. This correspondence is well-defined modulo $\mathcal{P}$ for a, b and c. The subgroup $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$ corresponds to a subspace, F, of V. Notice that if $W \in \Gamma\Gamma(\mathcal{P}^{n-1})$ then $W \equiv W^*$ modulo $\mathcal{P}^{n-1}$ for some $W^* \in \Gamma$.

Claim 3.6.1. *If $\Gamma(\mathcal{P}^n) < \Gamma$ then $\Gamma(\mathcal{P})/\Gamma(\mathcal{P}^{n-1})$ is a vector space V, and $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$ corresponds to a subspace, F. The action induced on V by conjugation by an element in $\Gamma\Gamma(\mathcal{P}^{n-1})$ preserves F.*

Proof. Conjugation preserves V as $\Gamma(\mathcal{P}^{n-1})$ and $\Gamma(\mathcal{P}^n)$ are normal subgroups of $\mathrm{PSL}_2(\mathcal{O}_d)$. Moreover, any conjugate of $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$ is a subgroup of $\Gamma(\mathcal{P}^{n-1})$. So it suffices to see that any conjugate of $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$ by an element of $\Gamma\Gamma(\mathcal{P}^{n-1})$ is a subgroup of Γ. Such an element is of the form XY for some X in Γ and Y in $\Gamma(\mathcal{P}^{n-1})$. The X conjugate of $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$ is clearly in Γ, and hence in $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$. Finally, since $\Gamma(\mathcal{P}^{n-1})/\Gamma(\mathcal{P}^n)$ is abelian, conjugating by Y preserves $\Gamma \cap \Gamma(\mathcal{P}^{n-1})$ modulo $\mathcal{P}^n$.

□

We will show this action explicitly. Given $M \in \Gamma \cap \Gamma(\mathcal{P}^{n-1})$ there is a $U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in M_2(\mathcal{O}_d)$ such that

$$M = I + q^{n-1}U.$$

Let $W = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_d)$. The action of conjugating M by W, $M \to WMW^{-1}$, interpreted in V sends the vector $u = (u_1, u_2, u_3)$ to the vector

$$W \cdot u = ([ad+bc]u_1 - acu_2 + bdu_3, -2abu_1 + a^2u_2 - b^2u_3, 2cdu_1 - c^2u_2 + d^2u_3).$$

By Lemma 3.6.1, if $u \in F$ then $W \cdot u \in F$. It will be uselful to calculate $W \cdot u$ for a few specific matrices. Let $a, b \in \mathcal{O}_d$ and define

$$M_{ab} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Conjugating M by M_{ab} takes $u = (u_1, u_2, u_3)$ to

$$\begin{aligned} M_{ab} \cdot u \;=\; & ([2ab-1]u_1 - au_2 + [ab^2 - b]u_3, \\ & [-2a^2b + 2a]u_1 + a^2u_2 + [-a^2b^2 2 + 2ab - 1]u_3, \\ & 2bu_1 - u_2 + b^2u_3). \end{aligned}$$

In particular,

$$M_{00} \cdot u = -(u_1, u_3, u_2),$$

$$M_{01} \cdot u = (-u_1 - u_3, -u_3, 2u_1 - u_2 + u_3)$$

and

$$M_{12} \cdot u = (3u_1 - u_2 + 2u_3, -2u_1 + u_2 - 5u_3, 4u_1 - u_2 + 4u_3).$$

If $M_{ab} \in \Gamma\Gamma(\mathcal{P}^{n-1})$ then this action fixes F by Claim 3.6.1.

The remainder of the section will establish restrictions on F corresponding to restrictions that will arise from the existence of one-cusped congruence subgroups.

Claim 3.6.2. *Let Γ be as above. If $\Lambda(\Gamma \cap \Gamma(\mathcal{P}^{n-1})) = \Lambda(\Gamma(\mathcal{P}^n))$, then $(b_1 b_2, b_2^2, -b_1^2) \in F$ if and only if $b_1 = b_2 = 0$.*

In particular, neither $(0, 1, 0)$ nor $(0, 0, 1)$ are in F.

Proof. Let $q \in \mathcal{O}_d$ be such that $(q) = \mathcal{P}$. Notice that for all

$$A = \begin{pmatrix} x & y \\ a_1 & a_2 \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_d),$$

$$A^{-1} \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} A = \begin{pmatrix} 1 + a_1 a_2 l & a_2^2 l \\ -a_1^2 l & 1 - a_1 a_2 l \end{pmatrix}.$$

So $(0, 0, 0)$ corresponds to the elements of the form

$$\begin{pmatrix} 1 + q^n a' & q^n b' \\ q^n c' & 1 + q^n d' \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_d)$$

under the identification modulo $\Gamma(\mathcal{P}^n)$. Any matrix of this form is in $\Gamma(\mathcal{P}^n) < \Gamma \cap \Gamma(\mathcal{P}^{n-1})$.

So it suffices to show that if $(b_1b_2, b_2^2, -b_1^2) \in F$ then $b_1 = b_2 = 0$. In the case where $b_1 = 0$ we have $(0, b_2^2, 0) \in F$, implying that

$$\begin{pmatrix} 1 & b_2^2 q^{n-1} \\ 0 & 1 \end{pmatrix} \in \Gamma \cap \Gamma(\mathcal{P}^{n-1}).$$

As $\Lambda(\Gamma \cap \Gamma(\mathcal{P}^{n-1})) = \Lambda(\Gamma(\mathcal{P}^n))$ we conclude that $b_2^2 q^{n-1} \equiv 0 \mod \mathcal{P}^n$. So $b_2^2 \equiv 0 \mod \mathcal{P}$ and hence $b_2 \equiv 0 \mod \mathcal{P}$. If $b_2 = 0$ then $(0, 0, -b_1^2) \in F$, corresponding to

$$\begin{pmatrix} 1 & 0 \\ -b_1^2 q^{n-1} & 1 \end{pmatrix} \in \Gamma \cap \Gamma(\mathcal{P}^{n-1}).$$

Again we conclude that $b_1 \equiv 0 \mod \mathcal{P}$. So under the correspondence, both b_1 and b_2 are zero.

We now assume that neither b_1 nor b_2 is zero. Let $k \in \mathcal{O}_d$ be such that $(k) = (b_1, b_2)$. Let a_i be such that $b_i = ka_i$. Therefore, if $(b_1b_2, b_2^2, -b_1^2) \in F$ then

$$\begin{pmatrix} 1 + b_1b_2q^{n-1} & b_2^2 q^{n-1} \\ -b_1^2 q^{n-1} & 1 - b_1 b_2^{q-1} \end{pmatrix} \in \Gamma \cap \Gamma(\mathcal{P}^{n-1})$$

and

$$\begin{pmatrix} 1 + b_1b_2q^{n-1} & b_2^2 q^{n-1} \\ -b_1^2 q^{n-1} & 1 - b_1b_2q^{n-1} \end{pmatrix} = A^{-1} \begin{pmatrix} 1 & k^2 q^{n-1} \\ 0 & 1 \end{pmatrix} A \in \Gamma \cap \Gamma(\mathcal{P}^{n-1})$$

for any

$$A = \begin{pmatrix} x & y \\ a_1 & a_2 \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_d).$$

As Γ has one cusp and all of the cusps of $\Gamma(\mathcal{P}^{n-1}) \cap \Gamma$ are conjugate in $\mathrm{PSL}_2(\mathcal{O}_d)$,

$$\begin{pmatrix} 1 & k^2 q^{n-1} \\ 0 & 1 \end{pmatrix} \in \Gamma \cap \Gamma(\mathcal{P}^{n-1}).$$

We conclude that since $\Lambda(\Gamma \cap \Gamma(\mathcal{P}^{n-1})) = \Lambda(\Gamma(\mathcal{P}^n))$ that $k^2 q^{n-1} \equiv 0 \mod \mathcal{P}^n$ and so $k \equiv 0 \mod \mathcal{P}$. So $(b_1, b_2) \subset (q)$ and thus $b_1 \equiv b_2 \equiv 0 \mod \mathcal{P}$. $\square$

The situation in the following proposition will occur frequently.

Proposition 3.6.3. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ lies over p and is not inert. Assume that*

$$\Lambda(\Gamma \cap \Gamma(\mathcal{P}^{n-1})) = \Lambda(\Gamma(\mathcal{P}^n)).$$

Then

i) There are s_1, $s_3 \in \mathbb{F}_p$ such that $(1, s_1, 0)$ and $(0, s_3, 1)$ form a basis for F.

ii) If $u = (u_1, u_2, u_3) \in F$ then $u_2 = u_1 s_1 + u_3 s_3$.

iii) If $p > 2$ then $s_1^2 - 4s_3$ is not a square in $\mathbb{F}_p$.

Proof. As they are linearly independent, it is sufficient to see that there are elements of the type $(a, b, 0)$ and $(0, \alpha, \beta)$ in F such that a, α and β are non-zero. If an element of the form $(a, b, 0)$ or $(0, \alpha, \beta) \in F$, then by Lemma 3.6.2 a, α, and β are non-zero. If no element of the form $(a, b, 0)$ were in F, then for all elements (x, y, z) and (x', y', z) in F, $x \equiv x'$, $y \equiv y'$. Therefore, for a fixed $z \in \mathbb{F}_p$ there would be a unique x, y such that $(x, y, z) \in F$, and so F would be one-dimensional. The case of $(0, \alpha, \beta)$ is similar.

For *ii*), if $u = (u_1, u_2, u_3) \in F$ there are $A, B, \in \mathbb{F}_p$ such that

$$u = (u_1, u_2, u_3) = A(1, s_1, 0) + B(0, s_3, 1) = (A, As_1 + Bs_3, B).$$

This implies that $u_1 = A, u_3 = B$ and so for all $(u_1, u_2, u_3) \in F$,

$$u_2 = u_1 s_1 + u_3 s_3.$$

To prove *iii*), notice that s_3 is non-zero since $(0, s_3, 1) \in F$, and $(0, 0, 1) \notin F$. Assume that $s_1^2 - 4s_3 \equiv l^2$ for some $l \in \mathbb{Z}_p$. It is enough to show that there is an $s \in \mathbb{F}_p$ such that

$$ss_1 - s^2 s_3 \equiv 1$$

as then

$$s(1, s_1, 0) - s^2(0, s_3, 1) = (s, ss_1 - s^2 s_3, -s^2) = (s, 1, -s^2) \in F$$

contradicting Claim 3.6.2. If $s_1 - 4s_3 \equiv l^2$, then since s_3 is non-zero we can write $l \equiv xs_3 - s_1$ for some $x \in \mathbb{F}_p$. So

$$l^2 \equiv s_1^2 + x^2 s_3^2 - 2xs_1 s_3 \equiv s_1^2 - 4s_3$$

and since s_3 is non-zero

$$2xs_1 - x^2 s_3 \equiv 4.$$

Setting $s = 2xy$ where $4y = 1$, we have $ss_1 - s^2 s_3 = 1$ as desired.

□

Chapter 4

Theorem 1.1.1

In this chapter, we will prove

Proposition 4.0.1. *There are finitely many maximal one-cusped congruence subgroups of the Bianchi Groups. Furthermore, any prime in $\mathcal{O}_d$ dividing the $\mathbb{Z}$-level of such a group has norm at most 11.*

If d =1, 2, or 7 there are finitely many one-cusped congruence subgroups of odd $\mathbb{Z}$-level, and if $d = 3$ there are finitely many one-cusped congruence subgroups of $\mathbb{Z}$-level relatively prime to 21.

If d =11, 19, 43, 67, or 163 there are finitely many one-cusped congruence subgroups of $\mathrm{PSL}_2(\mathcal{O}_d)$.

Unless $d = 3$ and p =3, or 7, or d =1, 2, or 7 and $p = 2$ the proof will produce explicit bounds on the maximal power of any prime p dividing the $\mathbb{Z}$-level of a one-cusped congruence subgroup. Proposition 4.0.1 implies Theorem 1.1.1 and the discussion following it.

In Section 4.2 we will prove

Proposition 4.0.2. (Prime $\mathbb{Z}$-Levels) *Let Γ be a one-cusped congruence subgroup of $\mathbb{Z}$-level p where p is a rational prime lying under a prime $\mathcal{P} \subset \mathcal{O}_d$.*

Then $N(\mathcal{P}) \leq 11$.

In Section 4.3 we will show

Proposition 4.0.3. (Prime Power $\mathbb{Z}$-Levels) *Let* Γ *be a one-cusped congruence subgroup of* $\mathbb{Z}$*-level* p^n*, where* p *is the rational prime lying under a prime* $\mathcal{P} \subset \mathcal{O}_d$*. Then* $N(\mathcal{P}) \leq 11$*. Moreover, unless* $p = 2$ *and is not inert,* $p = 3$ *is ramified or* $p = 7$ *and* $T(\Gamma) \neq 1$*, then*

$$n \leq \begin{cases} 0 & \text{if } N(\mathcal{P}) > 11, \text{ or } p = 3 \text{ is inert and } T(\Gamma) = 1 \\ 1 & \text{if } p = 7, 11 \text{ is ramified} \\ & \quad \text{or } p = 3 \text{ is inert and } T(\Gamma) \neq 1 \\ & \quad \text{or } p = 5, 11 \text{ is split} \\ & \quad \text{or } p = 7 \text{ is split and } T(\Gamma) = 1 \\ 2 & \quad \text{or } p = 3 \text{ is split} \\ & \quad \text{or } p = 2 \text{ is inert} \end{cases}$$

Assuming the above propositions, in Section 4.1 we will prove

Proposition 4.0.4. *Let* Γ *be a one-cusped congruence subgroup of* $\mathcal{O}_d$*-level* (n)*. Then* $N(\mathcal{P}) \leq 11$ *for all* $\mathcal{P}$ *dividing* (n)*.*

Deferring the proof of this proposition until Section 4.1, we will now complete the proof of Proposition 4.0.1. Let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ of $\mathbb{Z}$-level n. Since Γ has one cusp, $\mathcal{O}_d$ must have class number one, and therefore $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. By Lemma 4.0.4, if $\mathcal{P}$ is a prime in $\mathcal{O}_d$ dividing (n), then $N(\mathcal{P}) \leq 11$. Therefore, there is a finite set of primes, depending on d, such that the $\mathbb{Z}$-level of any one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ is only divisible by these primes.

Lemma 4.0.5. *Let* $\mathcal{O}_d$ *have class number one, let* $\mathcal{P}$ *be a non-zero prime in* $\mathcal{O}_d$*, with* $N(\mathcal{P}) \leq 11$*, and let* $p \in \mathbb{Z}$ *lie under* $\mathcal{P}$*. Then*

a) If p is not a split or ramified 2, ramified 3, or split 7 in $\mathcal{O}_3$ then there is a constant c_1 depending only on p and d such that there are no one-cusped congruence subgroups with p^{c_1} dividing the $\mathbb{Z}$-level

b) If p is a split or ramified 2, ramified 3, or split 7 in $\mathcal{O}_3$ then there is a constant c_1 depending only on p and d such that if p^{c_1} divides the $\mathbb{Z}$-level of a one-cusped congruence subgroup, Γ, then if $p = 7$, $\Gamma < \Gamma\Gamma(p)$ a one- cusped congruence subgroup of $\mathbb{Z}$-level p, and if $p \leq 3$ then $\Gamma < \Gamma\Gamma(p^2)$, a one- cusped congruence subgroup of $\mathbb{Z}$-level p^2.

Before we prove Lemma 4.0.5 we will complete the proof of Proposition 4.0.1. If d =11, 19, 43, 67, or 163, the prime 2 is inert and 3 is unramified. Therefore, by Lemma 4.0.5 a) and Proposition 4.0.4 the $\mathbb{Z}$-level of any one-cusped congruence subgroup divides

$$M = \prod p^{c_1(p,d)}$$

where the product is taken over the finite number of primes where $N(\mathcal{P}) \leq 11$ for all $\mathcal{P} \in \mathcal{O}_d$ lying over p. Therefore $\Gamma(M)$ is contained in all one-cusped congruence subgroups. As a result, there are only finitely many one-cusped congruence subgroups in $\mathcal{O}_{11}$, $\mathcal{O}_{19}$, $\mathcal{O}_{43}$, $\mathcal{O}_{67}$ or $\mathcal{O}_{163}$.

In $\mathcal{O}_1$, $\mathcal{O}_2$, and $\mathcal{O}_7$, the above argument shows that there are only finitely many one-cusped congruence subgroups of odd $\mathbb{Z}$-level. Moreover, if the $\mathbb{Z}$-level of a one-cusped congruence subgroup is even, then it divides $M2^n$ where

$$M = \prod p^{c_1(p,d)}$$

where the product is taken over the finite number of odd primes where $N(\mathcal{P}) \leq 11$ for all $\mathcal{P} \in \mathcal{O}_d$ lying over p. There are only finitely many of $\mathbb{Z}$-level dividing

$2^{c_1(2,d)}M$ and by Lemma 4.0.5 if Γ if $n > c_1(2,d)$ then such a subgroup is contained in a one-cusped congruence subgroup of $\mathbb{Z}$-level 4. This proves Proposition for d =1, 2 and 7. The proof in the case where $d = 3$ is analogous.

Proof. (proof of Lemma 4.0.5) Let p be a prime such that $N(\mathcal{P}) \leq 11$ for all primes $\mathcal{P} \subset \mathcal{O}_d$ lying over p. Notice that for any other prime $q \in \mathbb{Z}$ that the power of p dividing

$$M(q^n) = |\mathrm{SL}_2(\mathcal{O}_d/(q^n))| = \begin{cases} q^{3n-2}(q^2-1) & \text{if } q \text{ is not inert} \\ q^{6n-4}(q^4-1) & \text{if } q \text{ is inert} \end{cases}$$

is less than a constant, $c(p,q)$. Let

$$c_1(p,d) = 7 + \sum c(p,q)$$

where the sum is taken over all primes $q \in \mathbb{Z}$ such that $N(\mathcal{Q}) \leq 11$ for all primes $\mathcal{Q}$ lying over q.

Now assume that Γ is a one-cusped congruence subgroup of $\mathbb{Z}$-level n. If n is a prime power, Proposition 4.0.3 implies Lemma 4.0.5, so we will assume that n is composite. If p is a prime and p^t is the maximal power of a prime p dividing n, then let $n_1 = p^t$ and $n_2 = n/n_1$. Let $x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma]$ and $x_1 = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(n_1)]$. If ν_2 is the factor of the $\mathcal{O}_d$-level of Γ that is relatively prime to p, then

$$|N_1'| = \frac{x_1 M(\nu_2)}{x}$$

where N_1' is the group defined in Section 3.5 and $M(\nu_2) = |\mathrm{SL}_2(\mathcal{O}_d/\nu_2)|$. By the Index Lemma, p^{t-1} divides x. By the above discussion, since ν_2 divides (n_2), $M(\nu_2)$ divides $M(n_2)$ and therefore p^{c_1-7} does not divide $M(\nu_2)$. If $t > c_1$

we conclude that p^7 divides x_1. Therefore, $\Gamma\Gamma(n_1)$ is a one-cusped congruence subgroup of $\mathbb{Z}$-level a power of p. Since p^7 divides the index, we conclude that the $\mathbb{Z}$-level is at least p^3. In case a) this contradicts Proposition 4.0.3 and we conclude that the p^{c_1} cannot divide the $\mathbb{Z}$-level of a one-cusped congruence subgroup. In case b), by the Ladder Lemma, $\Gamma\Gamma(n_1)$ is a subgroup of $\Gamma\Gamma(p^2)$ which has $\mathbb{Z}$-level p if $p = 7$ and p^2 if $p = 2$ or 3. This completes the proof. $\square$

4.1 Composite $\mathbb{Z}$-Levels

We will first show

Lemma 4.1.1. *Let Γ be a one-cusped congruence subgroup of $\mathbb{Z}$-level m. Let p be the largest prime dividing m. Then $N(\mathcal{P}) \leq 11$ for all $\mathcal{P}$ in $\mathcal{O}_d$ lying over p.*

Next we will prove Proposition 4.0.4, that if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level (n), then $N(\mathcal{P}) \leq 11$ for all primes $\mathcal{P}$ dividing n.

4.1.1 Proof of Lemma 4.1.1

Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level (n). As $\mathcal{O}_d$ is a Dedekind domain,

$$(n) = \mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1}\dots\mathcal{P}_s^{\nu_s}$$

where $\mathcal{P}_i$ is a prime for $1 \leq i \leq s$ and $\mathcal{P}_i \neq \mathcal{P}_j$ for all $i \neq j$. Let p_i be the rational prime lying under $\mathcal{P}_i$, and order the $\mathcal{P}_i$ such that $p_i \geq p_{i-1}$. We will show that $N(\mathcal{P}_0) \leq 11$.

The Index Lemma states that if $\mathcal{P}_i$ is unramified, then $p_i^{\nu_i}$ divides $x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma]$, and if $\mathcal{P}_i$ is ramified then $p_i^{\lceil \frac{\nu_i}{2} \rceil}$ divides x, where $\lceil r \rceil$ is the ceiling function. By Proposition 4.0.2, we may assume that $s > 0$, and if $p_0 = p_1$ then $s > 1$.

We will use the notation established in Section 3.5. The approach will be to choose non-zero n_1 and $n_2 \in \mathcal{O}_d$ with $(n) = (n_1) \cap (n_2)$ and $(n_1, n_2) = \mathcal{O}_d$ such that there is a prime p dividing x but not $M(n_2) = |\mathrm{SL}_2(\mathcal{O}_d/(n_2))|$.

Therefore, as

$$|N_2'| = \frac{x_1 M(n_2)}{x},$$

p divides

$$x_1 = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(n_1)]$$

and hence $\Gamma\Gamma(n_1)$ is a proper one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$, whose $\mathcal{O}_d$-level divides (n_1). Notice that if p_0 is split with $\mathcal{P}_0\mathcal{P}_1 = (p_0)$ then $p_0 = p_1$. If n_2 is relatively prime to p_0, then as p_0 is chosen to be larger than any p_i dividing n_2, and since

$$M(n_2) = \prod_{\mathcal{P}_i | n_2} N(\mathcal{P}_i)^{3\nu_i - 2}(N(\mathcal{P}_i)^2 - 1)$$

we conclude that unless $p_0 = 3$ that p_0 can only divide $M(n_2)$ if it divides the factor $p_i^2 + 1$ corresponding to an inert p_i. We will assume that it is not the case that $p_0 = 3$ and $p_s = 2$ as here $N(\mathcal{P}_0) \leq 11$. We will break down the proof of Lemma 4.1.1 into four cases.

Case 1: Assume that $p_0 \neq p_1$ and p_0 does not divide $p_i^2 + 1$ for any inert p_i.

Let

$$(n_1) = \mathcal{P}_0^{\nu_0}$$

and

$$(n_2) = \mathcal{P}_1^{\nu_1}\mathcal{P}_2^{\nu_2}\ldots\mathcal{P}_s^{\nu_s}.$$

Since p_0 is the largest prime dividing $N(n)$, p_0 does not divide $M(n_2)$, as

$$M(n_2) = \prod_{j=2}^{s} N(\mathcal{P}_j)^{3\nu_j - 2}(N(\mathcal{P}_j)^2 - 1)$$

but p_0 does divide x by the Index Lemma. Therefore, p_0 divides x_1. So $\Gamma\Gamma(\mathcal{P}_0^{\nu_0})$ is a one-cusped subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ with $\mathcal{O}_d$- level a non-trivial power of the prime $\mathcal{P}_0$, and $N(\mathcal{P}_0) \leq 11$ by Proposition 4.3.

Case 2: Assume that $p_0 \neq p_1$ but p_0 divides $p_i^2 + 1$ for some inert p_i.

One can check that if $p_0 > 11$ is ramified, that p_0 does not divide $p_i^2 + 1$ for any inert p_i. Therefore we may assume that p_0 is unramified. First, we will show that if p_i and p_j are inert, $p_j < p_i < p_0$, and p_0 divides $p_i^2 + 1$, that p_0 does not divide $p_j^2 + 1$. Otherwise, we have

$$p_i^2 \equiv p_j^2 \equiv -1 \mod p_0.$$

Since $p_j, p_i < p_0$, and $p_i \neq p_j$ they are in different equivalence classes modulo p_0 and therefore,

$$p_j = -p_i \mod p_0$$

implying that $p_j = p_0 - p_i$. But p_0 and p_i are necessarily odd, so we conclude that $p_j = 2$ and therefore $p_0 = 5$ and $p_i = 3$. But the following lemma implies that in this case p_0 is split, and therefore $N(\mathcal{P}_0) = 5$.

Lemma 4.1.2. *Assume that $\mathcal{P}_0 = 5$, $\mathcal{P}_1 = 3$ and $\mathcal{P}_2 = 2$ are all inert. Then there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1}\mathcal{P}_2^{\nu_2}$, $\mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1}$, $\mathcal{P}_0^{\nu_0}\mathcal{P}_2^{\nu_2}$, or $\mathcal{P}_1^{\nu_1}\mathcal{P}_2^{\nu_2}$ if ν_0, ν_1, and ν_2 are positive.*

We will prove this after we have completed the proof of Case 2.

Continuing Case 2, if p_0^2 divides x, let

$$(n_1) = \mathcal{P}_0^{\nu_0}$$

and

$$(n_2) = \mathcal{P}_1^{\nu_1}\mathcal{P}_2^{\nu_2}\dots\mathcal{P}_s^{\nu_s}.$$

Using the notation in Section 3.5 recall that

$$|N_2'| = \frac{x_1 M(n_2)}{x}.$$

Since p_0^2 does not divide p_i^2+1 as $p_0 > p_i$, and p_0 does not divide p_j^2+1 for any other inert prime p_j, p_0^2 does not divide $M(n_2)$. As we are assuming p_0^2 divides x, we conclude that p_0 divides x_1 and $\Gamma\Gamma(\mathcal{P}_0^{\nu_0})$ has $\mathcal{O}_d$- level a non-trivial power of $\mathcal{P}_0$, so $N(\mathcal{P}_0) \leq 11$.

Therefore we may assume that p_0^2 does not divides x. By the Index Lemma, this implies that $\nu_0 = 1$ since $p_0 > 3$, and we let

$$(n_1) = \mathcal{P}_0\mathcal{P}_i^{\nu_i}.$$

Now p_0 divides x but not $M(n_2)$, so p_0 divides x_1. Therefore $\Gamma\Gamma(\mathcal{P}_0\mathcal{P}_i^{\nu_i})$ is a one-cusped congruence subgroup of $\mathcal{O}_d$- level $\mathcal{P}_0$ or $\mathcal{P}_0\mathcal{P}_i^{\omega_i}$ for some $1 \leq \omega_i \leq \nu_i$. In the first case, $N(\mathcal{P}_0) \leq 11$ by Proposition 4.0.2.

It now suffices to assume that $\Gamma\Gamma(\mathcal{P}_0\mathcal{P}_i^{\nu_i}) = \Gamma\Gamma(\mathcal{P}_0\mathcal{P}_i^{\omega_i})$ has $\mathcal{O}_d$-level $\mathcal{P}_0\mathcal{P}_i^{\omega_i}$ and p_0^2 does not divide $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_0\mathcal{P}_i^{\omega_i})]$. Abusing notation, let

$$(n) = \mathcal{P}_0\mathcal{P}_i^{\omega_i}, \quad (n_1) = \mathcal{P}_i^{\omega_i}, (n_2) = \mathcal{P}_0,$$

and

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_0\mathcal{P}_i^{\nu_i})].$$

We will prove the following two claims after we complete the proof of Case 2.

Claim 4.1.3. *$\mathcal{P}_0$ is not inert.*

Claim 4.1.4. *With p_0 and p_i as above, p_i does not divide $p_0 \pm 1$ unless $p_i = 2$ and $p_0 = 5$.*

Now, we see that p_i divides x by the Index Lemma, but not $M(n_2)$ which is $p_0(p_0+1)(p_0-1)$ since p_0 is not inert by Claim 4.1.3. Since $|N_2'| = x_1 M(n_2)/x$ we conclude that p_i divides x_1. Therefore $\Gamma\Gamma(\mathcal{P}_i^{\omega_i})$ has $\mathcal{O}_d$-level a non-trivial power of $\mathcal{P}_i$ and therefore $N(\mathcal{P}_i) \leq 11$. As we are assuming that p_i is inert, we conclude that p_i is 2 or 3 and therefore $p_0 = 5$ which is split by Claim 4.1.3.

Now we will prove Claims 4.1.2, 4.1.3, and 4.1.4.

Proof. (Proof of Lemma 4.1.2) Let $\mathcal{P}_5$ lie over 5, $\mathcal{P}_3$ lie over 3 and $\mathcal{P}_2$ lie over 2, and let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_5^{a_5}\mathcal{P}_3^{a_3}\mathcal{P}_2^{a_2}$.

First, assume that $a_5 = 0$. Let $(n_1) = \mathcal{P}_3^{a_3}$ and $(n_2) = \mathcal{P}_2^{a_2}$. By Proposition 4.3 $x_1 = 1$ as there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level a power of $\mathcal{P}_3$. Therefore

$$|N_2'| = \frac{x_1 M(n_2)}{x} = \frac{2^{6a_2-4} \cdot 3 \cdot 5}{x}$$

and we conclude that 3^2 does not divide x. By the Index Lemma we see that a_3 =1 or 2. If $a_3 = 1$ then as $\mathrm{PSL}_2(\mathbb{F}_9)$ is simple and

$$[\mathrm{SL}_2(\mathbb{F}_9) : N_1'] = \frac{x}{x_2}$$

we conclude that $N_1 = \{id\}$ or $\mathrm{PSL}_2(\mathbb{F}_9)$ and so $x = x_2, 2x_2, M(n_1)$ or $M(n_1)/2$. By the Index Lemma, 3 divides x, and 3 does not divide x_2 as in this case $d \neq 3$ and hence x_2 is a power of 2. Therefore $x \neq x_2$ or $2x_2$. But $M(n_1)$ cannot divide x as 5 divides $M(n_1)$ but not x, since x divides

$|\Lambda(\Gamma(\mathcal{P}_3^{a_3}\mathcal{P}_2^{a_2}))| = 3^{2a_3}2^{2a_2}$. Therefore $a_3 = 2$ but in this case as $\mathcal{P}_3$ and $\mathcal{P}_2$ are inert and 3^2 does not divide x, we see that 3^2 cannot divide either $\Lambda_1(\Gamma)$ or $\Lambda_\omega(\Gamma)$. Therefore $\Lambda(\Gamma(3\cdot 2^{a_2}))$ is contained in $\Lambda(\Gamma)$, contradicting the fact that $a_3 = 2$.

Now assume that $a_3 = 0$. Let $(n_1) = \mathcal{P}_5^{a_5}$ and $(n_2) = \mathcal{P}_2^{a_2}$. By Proposition 4.3 $x_1 = 1$ and as

$$|N_2'| = \frac{x_1 M(n_2)}{x} = \frac{2^{6a_2-4}\cdot 3\cdot 5}{x}$$

we conclude that 5^2 does not divide x. Therefore $a_5 = 1$ by the Index Lemma. As $\mathrm{PSL}_2(\mathbb{F}_{25})$ is simple and as

$$[\mathrm{SL}_2(\mathbb{F}_{25} : N_1'] = \frac{x}{x_2}$$

we conclude that $N_1 = \{id\}$ or $\mathrm{PSL}_2(\mathbb{F}_{25})$ and so $x = x_2$, $2x_2$, $x_2M(n_1)$ or $x_2M(n_1)/2$. The first two are impossible as 5 divides x by the Index Lemma, but not x_2, as any one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_2^{a_2}$ has index a power of 2. Similarly, the last two are impossible as 13 divides $M(n_1)$ but not x.

Now assume that $a_2 = 0$. Let $(n_1) = \mathcal{P}_5^{a_5}$ and $(n_2) = \mathcal{P}_3^{a_3}$. Therefore $x_1 = 1$ by Proposition 4.3, and

$$|N_2'| = \frac{x_1 M(n_2)}{x} = \frac{2^4\cdot 3^{6a_3-4}\cdot 5}{x}$$

and we conclude that 5^2 does not divide x. Therefore $a_5 = 1$ by the Index Lemma. We have

$$[\mathrm{SL}_2(\mathbb{F}_{25}) : N_1'] = \frac{x}{x_2}$$

and since $\mathrm{PSL}_2(\mathbb{F}_{25})$ is simple, we see that $x = x_2$, $2x_2$, $x_2M(n_1)$ or $M(n_1)$. As before, none of these is possible.

Finally, assume that none of a_5, a_3 or a_2 are zero. Let $(n_1) = \mathcal{P}_5^{a_5}\mathcal{P}_3^{a_3}$ and $(n_2) = \mathcal{P}_2^{a_2}$. So $x_1 = 1$ and as

$$|N_2'| = \frac{x_1 M(n_2)}{x} = \frac{2^{6a_2-4} \cdot 3 \cdot 5}{x}$$

we conclude that 5^2 does not divide x. Therefore $a_5 = 1$ by the Index Lemma and letting $(n_1) = \mathcal{P}_5$ and $(n_2) = \mathcal{P}_3^{a_3}\mathcal{P}_2^{a_2}$ we have a contradiction similar to above.

□

Proof. (Proof of Claim 4.1.3) We are assuming that $(n) = \mathcal{P}_0\mathcal{P}_i^{\omega_i}$, $\mathcal{P}_i$ is inert and p_0^2 does not divide x. Assume that $\mathcal{P}_0$ is inert. We will show that this is impossible.

Let $(n_1) = \mathcal{P}_0$ and $(n_2) = \mathcal{P}_i^{\omega_i}$, and recall that

$$|N_2'| = \frac{x_1 M(n_2)}{x}.$$

If $x_1 = 1$, then $N_1 \triangleleft \mathrm{PSL}_2(\mathcal{O}_d/\mathcal{P}_0)$ which is simple since $p_0 > 3$. Since

$$[\mathrm{SL}_2(\mathcal{O}_d/\mathcal{P}_0) : N_1'] = \frac{x}{x_2}$$

we conclude that $x = x_2$, $2x_2$, $M(n_1)x_2$ or $M(n_1)x_2/2$. The first two contradict the fact that p_0 divides x, and the second two imply that p_0^2 divides x. Therefore $x_1 \neq 1$ and $\Gamma\Gamma(\mathcal{P}_0)$ is a proper one-cusped congruence subgroup, implying that $N(\mathcal{P}_0) \leq 11$.. □

Proof. (Proof of Claim 4.1.4) We are assuming that p_0 divides p_i^2+1 and p_i divides $p_0 \pm 1$. So there are positive integers r and s such that

$$p_0 r = p_i^2 + 1, \text{and} p_i s = p_0 \pm 1.$$

We may assume that p_i is odd. (If $p_i = 2$ then $p_0 = 5$ and by Claim 4.1.2 p_0 is not inert.) By parity, we see that r is even. We have

$$p_0 r = p_i^2 + 1 = r(p_i s \mp 1).$$

If

$$p_0 r = p_i^2 + 1 = r(p_i s + 1),$$

then $p_i^2 = r p_i s + r - 1$ and therefore $r \leq p_i$. Also it implies that $r - 1 \equiv 0 \mod p_i$ and so $r = 1$. Hence, $p_0 = p_i^2 + 1$ which cannot occur by parity. If

$$p_0 r = p_i^2 + 1 = r(p_i s - 1)$$

then $p_i^2 = p_0 r - 1$ and so $r < p_i$. The right hand side, $p_i^2 + 1 = r(p_i s - 1)$ implies that $1 \equiv -r \mod p_i$ and therefore $r = p_i - 1$. We have $p_i^2 + 1 = (p_i - 1)(p_i s - 1)$ and so $p_i^2 = p_i^2 s - p_i - p_i s$ and $p_i = p_i s - 1 - s$ and we conclude that s cannot be 1 and $p_i = \frac{s+1}{s-1}$. Therefore, $p_i = 2$.

□

Case 3: Assume that $p_0 = p_1$ and p_0 does not divide $p_i^2 + 1$ for any inert $\mathcal{P}_i$ dividing (n).

Let

$$(n_1) = \mathcal{P}_0^{\nu_0} \mathcal{P}_1^{\nu_1},$$

and

$$(n_2) = \mathcal{P}_2^{\nu_2}\mathcal{P}_3^{\nu_3}\dots\mathcal{P}_s^{\nu_s}.$$

Here

$$|N_2'| = \frac{x_1 M(n_2)}{x}$$

and so p_0 divides x but not $M(n_2)$. Thus p_0 divides x_1 and $\Gamma\Gamma(\mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1})$ has $\mathcal{O}_d$- level $\mathcal{P}_0^{\omega_0}\mathcal{P}_1^{\omega_1}$ or, say, $\mathcal{P}_0^{\omega_0}$. In either case, the $\mathbb{Z}$-level is a power of p_0 and by Proposition 4.0.3, $N(\mathcal{P}_0) \leq 11$.

Case 4: Assume that $p_0 = p_1$ and p_0 divides $p_i^2 + 1$ for some inert $\mathcal{P}_i$ dividing (n).

We may assume that $p_0 > 3$. If p_0^2 divides x, then let $(n_1) = \mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1}$ and $(n_2) = \mathcal{P}_2^{\nu_2}\dots\mathcal{P}_s^{\nu_5}$. Therefore

$$|N_2'| = \frac{x_1 M(n_2)}{x}$$

and as p_0^2 does not divide $M(n_2)$, p_0 divides x_1 and so p_0 divides the $\mathbb{Z}$- level of $\Gamma\Gamma(\mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1})$. We conclude that $N(\mathcal{P}_0) \leq 11$. So assume that p_0^2 does not x and therefore $\nu_0 = \nu_1 = 1$ by the Index Lemma. Let

$$(n_1) = \mathcal{P}_0\mathcal{P}_1\mathcal{P}_i^{\nu_i}$$

and

$$(n_2) = \mathcal{P}_2^{\nu_2}\dots\mathcal{P}_{i-1}^{\nu_{i-1}}\mathcal{P}_{i+1}^{\nu_{i+1}}\dots\mathcal{P}_s^{\nu_s}.$$

Therefore p_0 divides x, but not $M(n_2)$.

By previous work, we may assume $\Gamma\Gamma(\mathcal{P}_0\mathcal{P}_1\mathcal{P}_i^{\nu_i})$ has $\mathcal{O}_d$- level $\mathcal{P}_0\mathcal{P}_1\mathcal{P}_i^{\omega_i}$ or $\mathcal{P}_0\mathcal{P}_i^{\omega_i}$ where $1 \leq \omega_i \leq \nu_i$. Abusing notation let $(n_1) = \mathcal{P}_i^{\omega_i}$, and $(n_2) = \mathcal{P}_0\mathcal{P}_1$ or $\mathcal{P}_0$, respectively. Therefore

$$|N_2'| = \frac{x_1 M(n_2)}{x}$$

and p_i divides x. Claim 4.1.4 implies that p_i does not divide $p_0(p_0+1)(p_0-1)$ unless $p_0 = 5$ and $p_i = 2$, so either $N(\mathcal{P}_i) \leq 11$ or p_i does not divide $M(n_2)$. Therefore $\Gamma\Gamma(\mathcal{P}_0\mathcal{P}_1\mathcal{P}_i^{\nu_i})\Gamma(\mathcal{P}_i^{\omega_i})$ has $\mathcal{O}_d$- level divisible by $\mathcal{P}_i$ and $N(\mathcal{P}_i) \leq 11$. So, $p_i = 2$ or 3 as it is inert, implying that $p_0 = 5$ and $N(\mathcal{P}_0) \leq 11$.

4.1.2 Proof of Proposition 4.0.4

We will prove that if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level (n) then $N(\mathcal{P}) \leq 11$ for all primes $\mathcal{P}$ dividing (n). We will need to recall the splitting types of small primes.

Table 4.1:
Splitting Types of Small Primes in $\mathcal{O}_d$, R=Ramified, S=Split and I=Inert

	$d=1$	2	3	7	11	19	43	67	163
$p=2$	R	R	I	S	I	I	I	I	I
3	I	S	R	I	S	I	I	I	I
5	S	I	I	I	S	S	I	I	I
7	I	I	S	R	I	S	I	I	I
11	I	S	I	S	R	S	S	I	I

It suffices to do a few calculations. As in the previous proof, let

$$(n) = \mathcal{P}_0^{\nu_0}\mathcal{P}_1^{\nu_1}\dots\mathcal{P}_s^{\nu_s}$$

be the $\mathcal{O}_d$- level of Γ with $\mathcal{P}_i$ lying over p_i, and ordered so that $p_i \geq p_{i+1}$. By Lemma 4.1.1 we know that $N(\mathcal{P}_0) \leq 11$. Therefore either $\mathcal{P}_0$ is split or

ramified and $p_0 \leq 11$ or $\mathcal{P}_0$ is inert and $p_0 = 2$ or 3. It suffices to rule out the possibility of having an inert prime $\mathcal{P}_i \neq \mathcal{P}_0$ such that $11 > p_i > 3$. We will call such a prime $\mathcal{P}$, lying over p, with ν the largest power of $\mathcal{P}$ dividing (n). The only possibilities are $p = 5$ or 7. If $p = 7$, notice that $(p, M(\mathcal{Q})) = 1$ for any other possible prime $\mathcal{Q}$ dividing (n). Therefore, if we let $(n_1) = \mathcal{P}^\nu$ then since p divides x by the Index Lemma, but not $M(n_2)$ using

$$|N_2'| = \frac{x_1 M(n_2)}{x}$$

we see that p divides x_1, resulting in a contradiction. Therefore it suffices to show that $p \neq 5$.

Table 4.2: $M(\mathcal{Q})$ for small primes $\mathcal{Q}$ in $\mathcal{O}_d$

	$N(\mathcal{Q}) = 2$	3	4	5	7	9	11	25
$M(\mathcal{Q})$	$2 \cdot 3$	$2^3 3$	$2^2 3 \cdot 5$	$2^3 3 \cdot 5$	$2^4 3 \cdot 7$	$2^4 3^2 \cdot 5$	$2^3 3 \cdot 5 \cdot 11$	$2^4 3 \cdot 5^2 13$

Notice that if (n) is coprime to $\mathcal{P}$ then $gcd(5, M(n)) = 1$ unless a split or ramified prime lying over 11 divides (n) or an inert 2 or 3 divides (n). Let (n_1) be the product of $\mathcal{P}^\nu$, with all the prime divisors, $\mathcal{P}'$, to their maximal powers such that $gcd(5, M(\mathcal{P}')) \neq 1$. Now 5 does not divide $M(n_2)$, but divides x by the Index Lemma. As

$$|N_1'| = \frac{x_1 M(n_2)}{x}$$

5 divides x_1 and therefore $\Gamma\Gamma(n_1)$ has $\mathcal{O}_d$- level divisible only by $\mathcal{P}$ and these $\mathcal{P}'$ such that $gcd(5, M(\mathcal{P})) \neq 1$. It now suffices to rule out these types of $\mathcal{O}_d$-levels.

Notice that when $d = 1$, 11 or 19 that 5 is split. When $d = 67$ or 163, the primes 5, 7 and 11 are all inert, so p_0 is either 2 or 3 by Lemma 4.1.1. As a result, we have proven Proposition 4.0.4 in these cases, and may assume that $d \in \{2, 3, 7, 43\}$.

We have Γ, a one-cusped congruence subgroup of $\mathcal{O}_d$-level (n), and $\mathcal{P}$ is prime lying over 5, with ν the largest power of $\mathcal{P}$ dividing (n). For a split prime lying over the prime $r \in \mathbb{Z}$, let $(r) = \mathcal{P}_r\mathcal{Q}_r$ where ν_r and μ_r are the powers of $\mathcal{P}_r$ and $\mathcal{Q}_r$ dividing (n). For an inert prime lying over r, let $(r) = \mathcal{P}_r$ with ν_r the power of $\mathcal{P}_r$ dividing (n).

In the $\mathcal{O}_2$ case, 2 is ramified, 3 and 11 are split, and 5 and 7 are inert. Therefore 5 only divides $M(\mathcal{Q})$ for those primes $\mathcal{Q}$ lying over 11. First, assume that Γ has $\mathcal{O}_d$-level $\mathcal{Q}_{11}^{\nu_{11}}\mathcal{P}^{\nu}$. Let $(n_1) = \mathcal{P}^{\nu}$ and $(n_2) = \mathcal{Q}_{11}^{\nu_{11}}$. Therefore $x_1 = 1$ and

$$|N_2'| = \frac{x_1 M(n_2)}{x} = \frac{M(n_2)}{x}.$$

Since 5^2 does not divide $M(n_2)$ we see that 5^2 does not divide x, and we conclude that $\nu = 1$ by the Index Lemma. Since

$$[\mathrm{SL}_2(\mathbb{F}_{25}) : N_1'] = \frac{x}{x_2}$$

and $N_1 \triangleleft \mathrm{PSL}_2(\mathbb{F}_{25})$ we conclude that $x = x_2$, $2x_2$, $M(n_2)$ or $M(n_2)/2$ and have a contradiction as 5 divides x but not x_2 and 3 divides $M(n_2)$ but not x.

Now assume that $(n) = \mathcal{P}_{11}^{\nu_{11}}\mathcal{Q}_2^{\mu_{11}}\mathcal{P}^{\nu}$. Let $(n_1) = \mathcal{P}_{11}^{\nu_{11}}\mathcal{P}^{\nu}$ and $(n_2) = \mathcal{Q}_{11}^{\mu_{11}}$. By above, $x_1 = 1$ or a power of 11. Since

$$|N_2'| = \frac{x_1 M(n_2)}{x}$$

and 5^2 does not divide $M(n_2)$ we conclude that 5^2 does not divide x and so $\nu = 1$ resulting in a contradiction as above.

In the $\mathcal{O}_3$ case, 11 is inert, 7 is split, 5 is inert, 3 is ramified, and 2 is inert. If $\mathcal{P}$ divides (n) then $\mathcal{P}_7$ or $\mathcal{Q}_7$ divides (n). Let $(n_1) = \mathcal{P}^\nu$ if $\mathcal{P}_2$ does not divide (n) or $\mathcal{P}^\nu\mathcal{P}_2^{\nu_2}$ if $\mathcal{P}_2$ divides (n). Then $\Gamma\Gamma(n_1)$ has $\mathcal{O}_d$-level dividing $\mathcal{P}^\nu\mathcal{P}_2^{\nu_2}$ with $\nu \geq 1$ since 5 does not divide $M(\mathcal{P}_7)$ or $M(\mathcal{P}_3)$. This is impossible by Lemma 4.1.2.

In $\mathcal{O}_7$ and $\mathcal{O}_{11}$, since 5^2 does not divide $M(\mathcal{Q})$ for any of the other primes $\mathcal{Q}$ that can divide (n), we can rule out the possibility that $(n) = \mathcal{P}^\nu\mathcal{Q}^\mu$ for any of these as we have done above. Then as above we can rule out $(n) = \mathcal{P}^\nu\mathcal{Q}^\mu\mathcal{R}^\omega$ where $\mathcal{R}$ is another prime. In this manner, we can show that $\mathcal{P}$ does not divide (n).

4.2 Prime $\mathbb{Z}$-Levels

In this section we prove Proposition 4.0.2, that if Γ is a one-cusped congruence subgroup of $\mathbb{Z}$-level p where p is a rational prime lying under $\mathcal{P} \subset \mathcal{O}_d$ then $N(\mathcal{P}) \leq 11$. We will do so with three lemmas. If the $\mathbb{Z}$-level os p for an inert prime, then the $\mathcal{O}_d$-level is (p). If p is split as $\mathcal{P}_1\mathcal{P}_2$ then the $\mathcal{O}_d$-level is $\mathcal{P}_1\mathcal{P}_2$, $\mathcal{P}_1$ or $\mathcal{P}_2$. If p is ramified with $\mathcal{P}$ lying over p, then the $\mathcal{O}_d$-level is either $\mathcal{P}$ or $\mathcal{P}^2$. First, in Section 4.2.1 we will show

Lemma 4.2.1. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}$ for a prime $\mathcal{P} \in \mathcal{O}_d$, then $N(\mathcal{P}) \leq 11$.*

This proves Proposition 4.0.2 for inert primes. Next, in Section 4.2.2 we prove

Lemma 4.2.2. *Let $p = \mathcal{P}_1\mathcal{P}_2$ be a split prime, and Γ a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_1\mathcal{P}_2$. If $p > 3$ then $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^2$ and $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$. Moreover, if $p \leq 3$ and $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^2$ then $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$ for $i = 1$ and 2.*

(A discussion of the term $T(\Gamma)$ is contained in Section 1.4.) This proves Proposition 4.0.2 for split primes. Finally, in Section 4.2.3 we show

Lemma 4.2.3. *Let n be a positive integer. There are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is a ramified prime and $N(\mathcal{P}) > 11$.*

which proves Proposition 4.0.2 for ramified primes. Together, Lemmas 4.2.1, 4.2.1 and 4.2.3 prove Proposition 4.0.2.

4.2.1 Prime $\mathcal{O}_d$-level

Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}$, let p be the rational prime lying under $\mathcal{P}$, and let $\{1, \omega\}$ be an integral basis for $\mathcal{O}_d$. Since $\mathcal{O}_d$ is a PID, $\mathcal{P} = (q)$ for some $q \in \mathcal{O}_d$. As $\Gamma(\mathcal{P}) < \Gamma$, $\Lambda(\Gamma(\mathcal{P})) \subset \Lambda(\Gamma)$, and hence $|\Lambda(\Gamma)|$ divides $|\Lambda(\Gamma(\mathcal{P}))|$. Notice that $|\Lambda(\Gamma)| \neq 1$ as this would imply that $\Lambda(\Gamma)$ is generated by 1 and ω and so by Wohlfahrt's Theorem $\Gamma(1) = \mathrm{PSL}_2(\mathcal{O}_d) < \Gamma$. As $\Lambda(\Gamma(\mathcal{P}))$ is generated by q and ωq, $|\Lambda(\Gamma(\mathcal{P}))| = N(\mathcal{P})$. So

$$|\Lambda(\Gamma)| = \begin{cases} p & \text{if } p \text{ is split or ramified} \\ p \text{ or } p^2 & \text{if } p \text{ is inert.} \end{cases}$$

Recall that

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)|\Lambda(\Gamma)|.$$

Therefore

$$x = \begin{cases} T(\Gamma)p & \text{if } p \text{ is split or ramified} \\ T(\Gamma)p^2 & \text{if } p \text{ is inert.} \end{cases}$$

As $\Gamma(\mathcal{P}) < \Gamma$, reduction modulo $\Gamma(\mathcal{P})$ sends Γ to an index x subgroup of

$$\mathrm{PSL}_2(\mathcal{O}_d)/\Gamma(\mathcal{P}) \cong \mathrm{PSL}_2(\mathbb{F}_{N(\mathcal{P})}).$$

A famous theorem of Galois [25] states that the smallest index of a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_r)$ is $r + 1$ except for r =2, 3, 5, 7, 9, or 11. When r =2, 3 ,5 ,7 or 11 the smallest index is r, and when $r = 9$ the smallest index is 6. Therefore, we have proven Lemma 4.2.1 in the case where $T(\Gamma) = 1$, as in this case x divides $N(\mathcal{P})$. Also, if p is inert and $|\Lambda(\Gamma)| = p$ we conclude that $p =$ 2 or 3 as x divides $T(\Gamma)p$, which is less than $N(\mathcal{P})$. So it remains to consider the case when $|\Lambda(\Gamma)| = T(\Gamma)N(\mathcal{P})$ and $T \in \{2, 3\}$. By the classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_r)$ [25] we conclude that if $T = 2$ (since $d = 1$), that

$N(\mathcal{P})$ =2,5, or 9 and if $T = 3$ (since $d = 3$), that $N(\mathcal{P})$ =3,4,7, or 19. And so $N(\mathcal{P}) \leq 11$ unless $p = 19$, $d = 3$ and $T(\Gamma) = 3$. Therefore it suffices to show that there are no one-cusped congruence subgroups, Γ, of $\mathcal{O}_3$-level $\mathcal{P}$ with $\mathcal{P}$ lying over $p = 19$ and

$$x = [\mathrm{PSL}_2(\mathcal{O}_3) : \Gamma] = 3 \cdot 19$$

.

Assume Γ is as above. Since Γ has one cusp, no conjugate of

$$\beta = \pm \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$

is in Γ where

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

Recall that if Γ contained β, then the cusp would be a pillow cusp, and the area of the cusp of the truncated compact manifold M'_Γ would be one third of the area of a cusp of the same width that had no peripheral torsion, i.e. where the cusp is a torus. Therefore, if Γ contained such an element then Γ cannot have only one cusp. By Wohlfahrt's Theorem, we conclude that presence of such an element implies that Γ has 3 cusps.

Let ϕ be the reduction modulo $\Gamma(\mathcal{P})$ map. Since

$$|\mathrm{PSL}_2(\mathbb{F}_{19})| = \frac{19(19^2 - 1)}{2} = 3420,$$

the order of $|\phi_{\mathcal{P}}(\Gamma)|$ is 60, and therefore contains an element of order 3. The Sylow 3-subgroups of $\mathrm{PSL}_2(\mathbb{F}_{19})$ are isomorphic to $\mathbb{Z}_9$ [5, 24]. So since all Sylow subgroups are conjugate, all elements of order 3 are conjugate. And

$\phi(\Gamma)$ contains an element of order 3, and therefore must contain an element conjugate to $\phi(\beta)$. As a result, Γ contains a conjugate of β. So there are no one-cusped congruence subgroups of $\mathcal{O}_3$-level $\mathcal{P}$ where $N(\mathcal{P}) = 19$. This completes the proof of Lemma 4.2.1.

4.2.2 Split Primes

Now we will prove Lemma 4.2.2. Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_1\mathcal{P}_2$ and let q_1 and q_2 be such that $(q_1) = \mathcal{P}_1$ and $(q_2) = \mathcal{P}_2$. We will show that if $p > 3$ that $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^2$ and $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$. If $p = 2$ or 3 we will show that if $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^2$ then $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$.

Since $\Lambda(\Gamma(p))$ is generated by p and $p\omega$, $|\Lambda(\Gamma(p))| = p^2$. As a result, since $\Gamma(p) < \Gamma$

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p \mathrm{or} T(\Gamma)p^2.$$

Notice that if $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$, the index

$$x_i = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_i)] = T(\Gamma)p \mathrm{or} p$$

and

$$\Lambda(\Gamma\Gamma(\mathcal{P}_i)) = \{q_i, \omega q_i\}.$$

In this case, by Wohlfahrt's Theorem, $\Lambda(\Gamma) \subsetneq \Lambda(\Gamma\Gamma(\mathcal{P}_i))$, and therefore

$$|\Lambda(\Gamma\Gamma(\mathcal{P}_i))| < |\Lambda(\Gamma)|$$

and $|\Lambda(\Gamma)| = p^2$ implying that $x = T(\Gamma)p^2$.

As a result, if $p > 3$ it suffices to show that the $\mathcal{O}_d$-level of $\Gamma\Gamma(\mathcal{P}_i)$ is $\mathcal{P}_i$. We will assume that $p > 3$, and that $\Gamma\Gamma(\mathcal{P}_1) = \mathrm{PSL}_2(\mathcal{O}_d)$ and derive a

contradiction. We will use the notation from Section 3.5. Since $\rho_1 \circ \phi_p = \phi_{\mathcal{P}_1}$,

$$B_1 = \rho_1(\phi_p(\Gamma)) = \phi_{\mathcal{P}_1}(\Gamma)$$

and as $\phi_{\mathcal{P}_1}$ is the reduction modulo $\mathcal{P}_1$ map, this is also $\phi_{\mathcal{P}_1}(\Gamma\Gamma(\mathcal{P}_1))$. As we are assuming that $\Gamma\Gamma(\mathcal{P}_1) = \mathrm{PSL}_2(\mathcal{O}_d)$ the image of $\Gamma\Gamma(\mathcal{P}_1)$ surjects $\mathrm{PSL}_2(\mathbb{F}_p)$ under $\phi_{\mathcal{P}_1}$. Since $p > 3$, $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple. As $N_1 \triangleleft B_1$, $N_1 = \{id\}$ or $\mathrm{PSL}_2(\mathbb{F}_p)$, and so $|N_1| = 1$ or $M(\mathcal{P}_1)/2$, where we have defined $M(n) = |\mathrm{SL}_2(\mathcal{O}_d/(n))|$ for all non-zero $(n) \in \mathcal{O}_d$. Therefore $|N_1'| = 1$, 2, $M(\mathcal{P}_1)/2$ or $M(\mathcal{P}_1)$. Since

$$|N_1'| = \frac{x_2 M(\mathcal{P}_1)}{x}$$

we conclude that $x = x_2 M(\mathcal{P}_1)$, $x_2 M(\mathcal{P}_1)/2$, $2x_2$, or x_2. Since $\Gamma(p) < \Gamma$, $|\Lambda(\Gamma)|$ divides $|\Lambda(p)| = p^2$, and so x divides $T(\Gamma)p^2$, ruling out the first two cases. The second two imply that $|\Lambda(\Gamma)| = |\Lambda(\Gamma\Gamma(\mathcal{P}_2))|$, contradicting Wohlfahrt's Theorem. Therefore the $\mathcal{O}_d$-level of $\Gamma\Gamma(\mathcal{P}_1)$ cannot be $\mathcal{O}_d$. This shows that $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$, by symmetry.

Now let p =2 or 3, so $T(\Gamma)$ necessarily equals 1 as neither 2 nor 3 is split in $\mathcal{O}_1$ or $\mathcal{O}_3$. Assuming that $x = p^2$ we will show that the $\mathcal{O}_d$-level of $\Gamma(\mathcal{P}_i)$ is $\mathcal{P}_i$. If $p = 2$ then

$$|N_1'| = \frac{3x_2}{2}, \quad |N_2'| = \frac{3x_1}{2}$$

so $x_1 = x_2 = 2$ as $|N_1'|$ is an integer. If $p = 3$ then

$$|N_1'| = \frac{2^3 x_2}{3}, \quad |N_2'| = \frac{2^3 x_2}{3}$$

so $x_1 = x_2 = 3$, implying the result.

4.2.3 Ramified Primes

We will show that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is a ramified prime with norm greater than 11. Let $q \in \mathcal{O}_d$ be such that $(q) = \mathcal{P}$. If $N(\mathcal{P}) > 11$ there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}$ by Lemma 4.2.1. It suffices to show that there are none of $\mathcal{O}_d$-level $\mathcal{P}^2$ as by the Ladder Lemma, this implies that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^n$ for $n > 0$. Assume that Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^2$ with $N(\mathcal{P}) > 11$. Therefore $T(\Gamma) = 1$ as $d \neq 1$ or 3. Since $|\Lambda(\Gamma(\mathcal{P}^2))| = p^2$ and $\Lambda((\Gamma(\mathcal{P}^2)) \subset \Lambda(\Gamma)$, we see that $|\Lambda(\Gamma)|$ divides p^2. By Wohlfahrt's theorem it is not 1, therefore

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = p \text{ or } p^2.$$

Notice that $|\Lambda(\Gamma)|$ can equal p, for example when $\Lambda(\Gamma)$ is generated by $\{1, p\omega\}$.

First, assume that $x = p^2$. We will use a vector space argument, as discussed in Section 3.6. Here the vector space F corresponding to $\Gamma \cap \Gamma(\mathcal{P})$ modulo $\Gamma(\mathcal{P}^2)$ is one-dimensional as

$$[\Gamma(\mathcal{P}) : \Gamma \cap \Gamma(\mathcal{P})] = [\Gamma\Gamma(\mathcal{P}) : \Gamma] = p^2.$$

Since $M_{ij} \in \Gamma\Gamma(\mathcal{P})$ for all $i, j \in \mathcal{O}_d$, $M_{ij} \cdot u \in F$ for all $u \in F$. Let $u = (a, b, c)$ be a generator. If $a = 0$ then $M_{00} \cdot u = -(a, c, b) \in F$, implying that $b = \pm c$. But $M_{12} \cdot (0, b, b) = (b, -4b, 3b) \in F$, which cannot occur as it implies that $b = 0$. Also $M_{12} \cdot (0, b, -b) = (-3b, 6b, -5b) \in F$, also implying $b = 0$ in this case. Therefore $a \neq 0$, and $M_{00} \cdot u = -(a, c, b) \in F$ and so $b = c$. But $M_{01} \cdot (a, b, b) = -(a + b, b, -2a)$, and so $(a + b, b, -2a) \in F$. So $2a = -b$.

Therefore $b \neq 0$ and hence $(a, b, b) = (a + b, b, -2a)$ implying that $a + b = a$. Therefore we see that $b = 0$ and $a = 0$, which is not possible.

Therefore, $x = p$.

Claim 4.2.4. *In this case,* $\mathrm{PSL}_2(\mathbb{Z}) < \Gamma$.

We will defer the proof of the claim until after we have completed the proof of Lemma 4.2.3.

If $\mathrm{PSL}_2(\mathbb{Z}) < \Gamma$, $\Lambda(\Gamma)$ is generated by 1 and ωp. Since $\Lambda(\Gamma(\mathcal{P}))$ is generated by q and ωq, we see that $\Lambda(\Gamma(\mathcal{P}) \cap \Gamma)$ is generated by p and ωp. By assumption $\Gamma\Gamma(\mathcal{P}) = \mathrm{PSL}_2(\mathcal{O}_d)$,

$$[\Gamma(\mathcal{P}) : \Gamma \cap \Gamma(\mathcal{P})] = [\Gamma\Gamma(\mathcal{P}) : \Gamma] = p.$$

Therefore, $\Gamma \cap \Gamma(\mathcal{P})$ corresponds to a two-dimensional subspace, F, of $\mathbb{Z}_{p^3}$ and satisfies the hypotheses of Proposition 3.6.3. Therefore

i) There are s_1, $s_3 \in \mathbb{F}_p$ such that $(1, s_1, 0)$ and $(0, s_3, 1)$ form a basis for F.

ii) If $u = (u_1, u_2, u_3) \in F$ then $u_2 = u_1 s_1 + u_3 s_3$.

iii) $s_1^2 - 4s_3$ is not a square in $\mathbb{F}_p$.

As $\Gamma\Gamma(\mathcal{P}) = \mathrm{PSL}_2(\mathcal{O}_d)$, $M_{ij} \in \Gamma\Gamma(\mathcal{P})$ for all $i, j \in \mathcal{O}_d$. So for all $u \in F$, $M_{ij} \cdot u \in F$. Specifically, $M_{00} \cdot (1, s_1, 0) = -(1, 0, s_1) \in F$. As $u_2 = u_1 s_1 + u_3 s_3$, we conclude that $0 = s_1(s_3 + 1)$ and so $s_1 = 0$ or $s_3 = -1$. Now $M_{00} \cdot (0, s_3, 1) = -(0, 1, s_3) \in F$, so $1 = s_3^2$. As a result, $s_3 = \pm 1$. Since $s_1^2 - 4s_3$ is not a square,

$$s_1 = 0 \text{ and } s_3 = 1, \text{ or } s_3 = -1.$$

Furthermore, $M_{12} \cdot (1, s_1, 0) = (3 - s_1, -2 + s_1, 4 - s_1) \in F$. If $s_1 = 0$ and $s_3 = 1$, we have $u_2 \equiv u_3$ and therefore $6 \equiv 0 \mod p$, a contradiction as $p > 3$. If $s_3 = -1$, this gives $s_1^2 - 3s_1 + 2 = 0$. Finally, $M_{12} \cdot (0, s_3, 1) = (-s_3 + 2, s_3 - 5, -s_3 + 4) = (3, -6, 5) \in F$, and so $-1 = 3s_1$. As a result, $s_1^2 = -3$, but then $s_1^2 - 4s_3 = 1$, which is a square. Therefore $x \neq p$. This completes the proof.

Proof. (Proof of Claim 4.2.4) We will prove that if $x = p$ then $\mathrm{PSL}_2(\mathbb{Z}) < \Gamma$. Let ϕ be the reduction modulo $\mathcal{P}^2$ map and let $\Gamma_z = \Gamma \cap \mathrm{PSL}_2(\mathbb{Z})$. First, we will show that $\phi(\Gamma_z) = \phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}))$. To see this it suffices to show that

$$\phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}) < \phi(\Gamma \cap \mathrm{PSL}_2(\mathbb{Z})).$$

If $\alpha \in \phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}))$ we have $\alpha = \phi(\gamma) = \phi(\beta)$ for some $\gamma \in \Gamma \text{and} \beta \in \mathrm{PSL}_2(\mathbb{Z})$. Since $\phi(\gamma) = \phi(\beta)$, $\gamma \equiv \beta \mod \mathcal{P}^2$ and so $\beta = \gamma M$ for some $M \in \Gamma(\mathcal{P}^2)$. Therefore $\beta \in \Gamma$ since $M \in \Gamma(\mathcal{P}^2) < \Gamma$ and therefore $\alpha = \phi(\beta)$ for $\beta \in \Gamma \cap \mathrm{PSL}_2(\mathbb{Z})$.

Notice that

$$[\phi(\mathrm{PSL}_2(\mathbb{Z})) : \phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}))] \leq [\phi(\mathrm{PSL}_2(\mathcal{O}_d)) : \phi(\Gamma)] = p$$

and as $p > 11$ there are no subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$ of index less than $p+1$. So

$$\phi(\mathrm{PSL}_2(\mathbb{Z})) = \phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z})) < \phi(\Gamma)$$

Since $\phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z})) < \phi(\Gamma)$ we conclude that

$$\phi(\Gamma \cap \mathrm{PSL}_2(\mathbb{Z})) = \phi(\mathrm{PSL}_2(\mathbb{Z}))$$

and since $\ker\phi < \Gamma$ we conclude that $\mathrm{PSL}_2(\mathbb{Z}) < \Gamma$. □

4.3 Prime Power $\mathbb{Z}$-Levels

In this section we will prove Proposition 4.0.3. We assume that Γ is a one-cusped congruence subgroup of $\mathbb{Z}$-level p^n, where p is a rational prime lying under a prime $\mathcal{P} \subset \mathcal{O}_d$. If $p = 2$ then we assume that p is inert, if $p = 3$ we assume it is unramified, and if $p = 7$ we assume that $T(\Gamma) = 1$. Then we prove that $N(\mathcal{P}) \leq 11$ and there is a constant $c_1(d, \mathcal{P})$ such that $n \leq c_1$. We will prove this by dealing with each prime splitting type separately. We have shown in the proof of Proposition 4.0.2 that there are no one-cusped subgroups of $\mathbb{Z}$-level any power of a ramified prime of norm greater than 11. Therefore the following three lemmas will suffice. In Section 4.3.1 we will prove

Lemma 4.3.1. (Ramified Primes) *Let p be a ramified prime such that $\mathcal{P}$ lies over p and let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$. Then*

$$n \leq \begin{cases} 1 & p = 7, 11 \\ 0 & p > 11. \end{cases}$$

This proves Proposition 4.0.3 for ramified primes. If p is an inert prime lying over $\mathcal{P}$ and $p > 3$, the Ladder Lemma implies that if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$, then $\Gamma\Gamma(\mathcal{P})$ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}$. By Proposition 4.0.2, $N(\mathcal{P}) \leq 11$, so $p \leq 3$. So for inert primes, the following lemma which will be proven in Section 4.3.2 will suffice.

Lemma 4.3.2. (Inert Primes) *Let p be an inert prime such that $\mathcal{P}$ lies over p. Let Γ be a one-cusped congruence subgroup of $\mathbb{Z}$-level p^n. Then*

$$n = \begin{cases} 1 \text{ or } 2 & p = 2 \text{ and } T(\Gamma) \neq 1 \\ 2 & p = 2 \text{ and } T(\Gamma) = 1 \\ 1 & p = 3 \text{ and } T(\Gamma) \neq 1 \\ 0 & p > 3 \text{ or } p = 3 \text{ and } T(\Gamma) = 1 \end{cases}$$

For a split prime, we prove the following in Section 4.3.3

Lemma 4.3.3. (Split Primes) *Let $p = \mathcal{P}\mathcal{Q}$ be a split prime and let Γ be a one-cusped congruence subgroup of $\mathbb{Z}$-level p^n. Assume $p \neq 2$ and if $p = 7$ that $T(\Gamma) = 1$. Then*

$$n \leq \begin{cases} 2 & p = 3 \\ 1 & p = 5, 11 \text{ or } p = 7 \text{ and } T(\Gamma) = 1 \\ 0 & p > 11. \end{cases}$$

4.3.1 Powers of Ramified Primes

In Lemma 4.2.3 we proved that the if the $\mathcal{O}_d$-level of Γ is $\mathcal{P}^n$ where $\mathcal{P}$ is a ramified prime, then $N(\mathcal{P}) \leq 11$. If $\mathcal{P}$ lies over p and $N(\mathcal{P}) \leq 11$ then the possibilities are

$$p = \begin{cases} 2 & \text{and } d = 1 \text{ or } 2 \\ 3 & \text{and } d = 3 \\ 7 & \text{and } d = 7 \\ 11 & \text{and } d = 11. \end{cases}$$

We will show that if $p = 7$ or 11 then $n = 1$.

Lemma 4.3.4. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is ramified lying over 7 or 11. Then $n = 1$.*

Proof. By the classification theorem of subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$ for $p = 7$ and 11 there is a subgroup, H, of index p in $\mathrm{PSL}_2(\mathbb{F}_p)$ [25] and $\phi^{-1}(H)$ necessarily has one cusp by Wohlfahrt's theorem. In fact, $\mathrm{PSL}_2(\mathbb{F}_{11})$ has two conjugacy classes of index 11 subgroups and $\mathrm{PSL}_2(\mathbb{F}_7)$ has two conjugacy classes of index 7 subgroups [5], [24]. It is sufficient to show that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^2$ or $\mathcal{P}^3$.

Claim I: There are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^2$.

Assume that Γ is such a group. Then as $d = 7$ or 11, $T(\Gamma) = 1$ and

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = p \text{ or } p^2.$$

Let $(q) \in \mathcal{O}_d$ be such that $(q) = \mathcal{P}$.

Case 1: $x = p$

Since $x = p$, $\Gamma\Gamma(\mathcal{P})$ is necessarily $\mathrm{PSL}_2(\mathcal{O}_d)$. We will use a vector space argument as discussed in Section 3.6. Recall that $\Gamma(\mathcal{P})/\Gamma(\mathcal{P}^2)$ is a three -dimensional vector space over $\mathbb{F}_p$. Under this correspondence, $\Gamma \cap \Gamma(\mathcal{P})$ corresponds to a two-dimensional subspace, F as

$$[\Gamma(\mathcal{P}) : \Gamma \cap \Gamma(\mathcal{P})] = p.$$

Since $x = p$, $\Lambda(\Gamma)$ is generated by $\{p, \omega + x\}$ or $\{\omega p, 1 + \omega y\}$ for some x and y in $\mathbb{Z}$. The lattice $\Lambda(\Gamma(\mathcal{P}))$ is generated by $\{q, \omega q\}$. As a result, $\Lambda(\Gamma) \neq \Lambda(\Gamma \cap \Gamma(\mathcal{P}))$. Since $\Gamma(\mathcal{P}^2) < \Gamma \cap \Gamma(\mathcal{P}^2)$, $\Lambda(\Gamma(\mathcal{P}^2)) \subset \Lambda(\Gamma \cap \Gamma(\mathcal{P}))$. Similarly, $\Lambda(\Gamma \cap \Gamma(\mathcal{P}^2))$ is contained in both $\Lambda(\Gamma)$ and $\Lambda(\Gamma(\mathcal{P}))$. As $|\Lambda(\Gamma)| = |\Lambda(\Gamma(\mathcal{P}))| = p$ and $|\Lambda(\Gamma(\mathcal{P}^2))| = p^2$ we conclude that $\Lambda(\Gamma \cap \Gamma(\mathcal{P}))$ is generated by p and ωp. Therefore we are in the situation of Proposition 3.6.3.

i) There are s_1, $s_3 \in \mathbb{F}_p$ such that $(1, s_1, 0)$ and $(0, s_3, 1)$ form a basis for F.

ii) If $u = (u_1, u_2, u_3) \in F$ then $u_2 = u_1 s_1 + u_3 s_3$.

iii) $s_1^2 - 4s_3$ is not a square in $\mathbb{F}_p$.

As $\Gamma\Gamma(\mathcal{P}) = \mathrm{PSL}_2(\mathcal{O}_d)$, $M_{00} \in \Gamma\Gamma(\mathcal{P})$ and we conclude that

$$s_1 = 0 \text{ and } s_3 = 1, \text{ or } s_3 = -1.$$

Additionally, $M_{12} \in \Gamma\Gamma(\mathcal{P})$. Notice that $(1, s_1, 0) \cdot M_{00} = -(1, 0, s_1) \in F$. If $s_1 = 0$ and $s_3 = 1$ then the generators are $(1, 0, 0)$ and $(0, 1, 1)$, and $M_{12} \cdot (0, 1, 1) = (1, -4, 3) \in F$, which is not in the span. Therefore $s_3 = -1$, and the generators are $(1, s_1, 0)$ and $(0, -1, 1)$. Now $M_{12} \cdot (0, -1, 1) = (3, -6, 5) \in F$. Therefore $3s_1 - 5 \equiv -6$ and we conclude that $3s_1 = -1$. Finally, $M_{12} \cdot (1, s_1, 0) = (3-s_1, -2+s_1, 4-s_1) \in F$. Therefore $(9-3s_1, -6+3s_1, 12-3s_1) = (10, -7, 13) \in F$ and we conclude that $10s_1 = 6$. Since $3s_1 = -1$ this implies that $30s_1 = 10(-1) = 18$, which is impossible as $p = 7$ or 11. Therefore $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] \neq p$.

Case 2: $x = p^2$.

Since $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = p^2$, $\Lambda(\Gamma) = \{p, \omega p\}$. We have two cases, either the $\mathcal{O}_d$-level of $\Gamma\Gamma(\mathcal{P})$ is $\mathcal{P}$ or is 1.

Subcase 1: The $\mathcal{O}_d$-level of $\Gamma\Gamma(\mathcal{P})$ is $\mathcal{P}$.

We will use the vector space technique as before with F corresponding to $\Gamma \cap \Gamma(\mathcal{P})$. Since $[\Gamma\Gamma(\mathcal{P}) : \Gamma] = p$, F is a two-dimensional subspace of $\mathbb{F}_p^3$. Again, by Proposition 3.6.3 we have

i) There are s_1, $s_3 \in \mathbb{F}_p$ such that $(1, s_1, 0)$ and $(0, s_3, 1)$ form a basis for F.

ii) If $u = (u_1, u_2, u_3) \in F$ then $u_2 = u_1 s_1 + u_3 s_3$.

iii) $s_1^2 - 4s_3$ is not a square in $\mathbb{F}_p$.

In $\mathrm{PSL}_2(\mathbb{F}_7)$ there are two conjugacy classes of index 7 subgroups, $\mathcal{A}$, and $\mathcal{B}$. A representative for $\mathcal{A}$ contains M_{00}, M_{1-1}, M_{-32}, and M_{42} and a representative for $\mathcal{B}$ contains M_{00}, M_{1-1}, and M_{-22}.[5, 24] As M_{00} is in each group, we conclude that

$$s_1 = 0 \text{ and } s_3 = 1, \text{ or } s_3 = -1.$$

Notice that $M_{-11} \cdot (1, s_1, 0) = (-3 - s_1, 4 + s_1, -2 - s_1)$. Therefore,

$$4 + s_1 = s_1(-3 - s_1) + s_3(-2 - s_1)$$

so we conclude that $s_3 = -1$ and hence

$$s_1^2 + 3s_1 + 2 = 0.$$

The only values for s_1 satisfying this in $\mathbb{F}_7$ are $s_1 = -1$ or -2, however, if $s_1 = -2$, $s_1^2 - 4s_3$ is a square. Therefore

$$s_1 = s_3 = -1$$

and the generators are $(1, -1, 0)$ and $(0, -1, 1)$. If $\Gamma\Gamma(\mathcal{P})$ corresponds to $\mathcal{A}$, then$(1, -1, 0) \cdot M_{-32} = (-2, -2, 5)$ which is not in the span of the basis vectors. And if $\Gamma\Gamma(\mathcal{P})$ corresponds to $\mathcal{B}$, $(1, -1, 0) \cdot M_{-22} = (-4, -3, 5)$ which in not in F.

In $\mathrm{PSL}_2(\mathbb{F}_{11})$ there are two conjugacy classes of index 11 subgroups, $\mathcal{C}$ and $\mathcal{D}$. A representative of $\mathcal{C}$ contains M_{00}, M_{1-1}, M_{3-4}, and M_{-33} and a representative of $\mathcal{D}$ contains M_{00}, M_{1-1}, M_{-32}, and M_{-44}. As M_{00} is in each group, we conclude that

$$s_1 = 0 \text{ and } s_3 = 1, \text{ or } s_3 = -1.$$

We have $M_{1-1} \cdot (1, s_1, 0) = (-3 - s_1, 4 + s_1, -2 - s_1)$ and hence

$$4 + s_1 = s_1(-3 - s_1) + s_1(-2 - s_1).$$

Therefore $s_3 = -1$ and

$$s_1^2 + 3s_1 + 2 = 0.$$

The only values satisfying this in $\mathbb{F}_{11}$ are $s_1 = -1$ or -2, but if $s_1 = -1$ then $s_1^2 - 4s_3$ is a square. Therefore $s_1 = -2$ and $s_3 = -1$. The generators are $(1, -2, 0)$ and $(0, -1, 1)$. If $\Gamma\Gamma(\mathcal{P})$ corresponds to $\mathcal{C}$ then we see that $M_{-33} \cdot (1, -2, 0) = (-3, -1, -3)$ which is not in the span of the basis vectors. For the group $\mathcal{D}$, $M_{-32} \cdot (1, -2, 0) = (3, 6, 6)$ which is not in the span. We conclude that $\Gamma\Gamma(\mathcal{P})$ does not have $\mathcal{O}_d$-level $\mathcal{P}$.

Subcase 2: The $\mathcal{O}_d$-level of $\Gamma\Gamma(\mathcal{P})$ is 1.

Therefore $\Gamma\Gamma(\mathcal{P})$ is $\mathrm{PSL}_2(\mathcal{O}_d)$ and as

$$[\Gamma\Gamma(\mathcal{P}) : \Gamma] = [\Gamma \cap \Gamma(\mathcal{P})] = p^2$$

under the vector space correspondence, $\Gamma \cap \Gamma(\mathcal{P})$ corresponds to a one - dimensional subspace, F. As before, $\Lambda(\Gamma \cap \Gamma(\mathcal{P}))$ is generated by p and ωp, and so neither $(0, 1, 0)$ nor $(0, 0, 1)$ is in F. Since F is one-dimensional, it is generated by one vector, u, of the form (a, b, c), specifically $(1, \beta, \gamma)$, or $(0, 1, \gamma)$. Notice that $M_{00} \cdot u \in F$ implies that $(1, \gamma, \beta)$, or $(0, \gamma, 1) \in F$, respectively. Therefore a generator u is of the form

$$(1, 0, 0), (0, 1, 1), (0, 1, -1), \text{or} (1, \beta, \beta)$$

where β is non-zero. Now

$$M_{12} \cdot u = (3, -2, 4), (1, -4, 3), (-3, 6, -5), \text{or} (3 + \beta, -2 - 4\beta, 4 + 3\beta)$$

respectively. This rules out the first three possibilities. For the final case, it implies that

$$(3+\beta, -2-4\beta, 4+3\beta) = (3+\beta)(1, \beta, \beta)$$

and therefore

$$-2-4\beta \equiv (3+\beta)\beta \mod \mathcal{P}$$

and since the last two entries are equal,

$$-2-4\beta \equiv 4+3\beta \mod \mathcal{P}.$$

Therefore $\beta^2 + 7\beta + 2 = 0$ and $6 \equiv -7\beta$. Immediately we see that $p \neq 7$. Substituting, we have $\beta^2 \equiv 4$, and therefore $\beta = \pm 2$. But $\pm 14 \not\equiv 6 \mod 11$, and therefore there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^2$.

Claim II: There are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^3$.

In this case $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = p^2$ or p^3 by the Index Lemma. By the Ladder Lemma $\Gamma\Gamma(\mathcal{P}^2)$ has $\mathcal{O}_d$-level $\mathcal{P}$ or $\mathcal{P}^2$. Since we have established that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^2$, $\Gamma\Gamma(\mathcal{P}^2) = \Gamma\Gamma(\mathcal{P})$ and has $\mathcal{O}_d$-level $\mathcal{P}$. Therefore as $\Gamma(\mathcal{P}^2)/\Gamma(\mathcal{P}^3)$ is a three-dimensional vector space over $\mathbb{F}_p$, and $\Gamma \cap \Gamma(\mathcal{P}^2)$ corresponds to a one or two-dimensional subspace. In the two-dimensional case this results in a contradiction as above since $\Lambda(\Gamma \cap \Gamma(\mathcal{P}^2)) = \Lambda(\Gamma(\mathcal{P}^3))$.

Assume that F is one-dimensional. Since $M_{00} \in \Gamma\Gamma(\mathcal{P}^2) = \Gamma\Gamma(\mathcal{P})$, we conclude that a generator u for F is of the form

$$(1,0,0), (0,1,1), (0,1,-1) \text{ or } (1,\beta,\beta).$$

The action of M_{1-1} takes the generators to

$$(-3,4,-2),(1,-4,0),(-3,6,-2), \text{ and } (-3+\beta,4-4\beta,-2),$$

respectively. This leaves only the final case, where the generator is $(1,\beta,\beta)$. We conclude that

$$(-3+\beta)(1,\beta,\beta) = (-3+\beta,4-4\beta,-2).$$

Since $4-4\beta=-2$ we see that $2\beta \equiv 3$. Also, since $\beta(-3+\beta)=-2$ we see that $2\beta^2=5$. This implies that $4\beta^2 \equiv 9$ and $4\beta^2 \equiv 10$, respectively.

□

4.3.2 Powers of Inert Primes

Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ for an inert prime $\mathcal{P}$. Let p be the rational prime lying under $\mathcal{P}$. We will show that

$$n = \begin{cases} 1 \text{ or } 2 & \text{if } p=2 \text{ and } T(\Gamma)\neq 1 \\ 2 & \text{if } p=2 \text{ and } T(\Gamma)=1 \\ 1 & \text{if } p=3 \text{ and } T(\Gamma)\neq 1 \\ 0 & \text{if } p=3 \text{ and } T(\Gamma)=1 \end{cases}$$

We will first assume that $p=2$ and next consider the case where $p=3$.

Lemma 4.3.5. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is inert and lies over 2. If $T(\Gamma)=1$, then $n=2$ and $[\mathrm{PSL}_2(\mathcal{O}_d):\Gamma]=16$. If $T(\Gamma)=3$, then $d=3$ and $n=1$ or 2.*

Proof. **Case I:** $T(\Gamma)=1$**.**

As

$$\mathrm{PSL}_2(\mathcal{O}_d)/\Gamma(\mathcal{P}) \cong \mathrm{PSL}_2(\mathbb{F}_4)$$

which has no subgroups of index 2 or 4, [5] there are no one-cusped subgroups of $\mathcal{O}_d$-level $\mathcal{P}$.

The following is a presentation for $\mathrm{PSL}_2(\mathcal{O}_3/(4))$, with generators a, b, and c corresponding to

$$a = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad c = \pm \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix},$$

and relations

$$\begin{array}{l} a^4, c^4, b^2, (ab)^3, aca^{-1}c^{-1} \\ (abcbacbac^{-1}bc^{-1}a^{-1}bc^{-1}b)^{-2} \\ (acbc^{-2}b)^2, (acbc^{-1}b)^3 \\ a^{-2}c^{-1}bcbc^{-1}bc^{-1}bcb \quad [10,\ 5] \end{array}$$

This is a presentation for $\mathrm{PSL}_2(\mathcal{O}_3)$ [10] with the additional relations a^4, c^4, and $(abcbacbac^{-1}bc^{-1}a^{-1}bc^{-1}b)^{-2}$. One can verify that it is a presentation for $\mathrm{PSL}_2(\mathcal{O}_3/(4))$ by verifying that the additional relations hold and seeing that the orders of the finite groups are equal. There are no subgroups of order 2,4, or 8. [5] There are subgroups of order 16 which can be seen to have one cusp by determining the corresponding lattices. Since $\mathcal{O}_3/(4) \cong \mathcal{O}_d/(4)$ for all other d with class number one when 4 is inert, we have shown in general that the only one-cusped congruence subgroups of $\mathcal{O}_d$-level (2) or (4) are these index 16 subgroups.

By the Ladder Lemma it suffices to show that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^3$. Let Γ be such a group, so $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 32$ or 64. Notice that by the Ladder Lemma $\Gamma\Gamma(4)$ must be one of the previously mentioned index 16 subgroups. In $\mathcal{O}_3$ there are 4 conjugacy classes of index 16 subgroups. [5] Each has only one conjugacy class of index

2 subgroups which contain

$$\pm \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 4\omega \\ 0 & 1 \end{pmatrix}.[5]$$

By Wohlfahrt's theorem, these cannot be one-cusped of $\mathcal{O}_3$-level $\mathcal{P}^3$. In addition, the four conjugacy classes of subgroups of index 16 all have two conjugacy classes of index 4 subgroups. These share the property that they either do not contain

$$\pm \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 8\omega \\ 0 & 1 \end{pmatrix},$$

or contain

$$\pm \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 4\omega \\ 0 & 1 \end{pmatrix}.[5]$$

This implies that they cannot be one-cusped congruence subgroup of $\mathcal{O}_3$-level $\mathcal{P}^3$ by Wohlfahrt's theorem. This shows that if $\mathcal{P}$ is inert and lies over 2 then there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}^n$ if $n > 2$ and $T(\Gamma) = 1$.

Case II: $T(\Gamma) \neq 1$**.**

Now we consider the case when Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ and $T(\Gamma) \neq 1$. Therefore $d = 3$ and Γ and so $T = 3$. First, we will consider subgroups of $\mathcal{O}_3$-level (2); such subgroups must have index 6 or 12. In $\mathrm{PSL}_2(\mathbb{F}_4)$ there is one conjugacy class of subgroups of index 6 and 12, [5] both of which by index considerations must have one cusp. Each index 12 subgroup is contained in an index 6 subgroup. [5] Therefore we have one-cusped congruence subgroups of $\mathcal{O}_3$-level (2) of index 6 and 12, Γ_6 and Γ_s. The group Γ_s corresponds to the fundamental group of the sister of the

figure-eight knot complement. Up to conjugation,

$$\Lambda(\Gamma_6) =< 1, 2\omega >$$

and

$$\Lambda(\Gamma_s) =< 2, 2\omega > .$$

If Γ has $\mathcal{O}_3$-level (4) then $[\mathrm{PSL}_2(\mathcal{O}_3) : \Gamma] = 3 \cdot 2^a$ where $a \in \{2, 3, 4\}$. By index considerations $\Gamma\Gamma(2)$ must be index 6 or 12 and therefore must be a subgroup of the index 6 subgroup, as otherwise the second isomorphism theorem implies that 3 divides $[\Gamma(2) : \Gamma \cap \Gamma(2)]$. By searching low index subgroups of $\mathrm{PSL}_2(\mathcal{O}_3/(4))$ we see that there are 3 conjugacy classes of index 12 subgroups. [5] One corresponds to Γ_s. The other two have $\mathcal{O}_3$-level (4), Γ_8, and, Γ_t. The group Γ_8 corresponds to the fundamental group of the figure-eight knot complement. The lattice $\Lambda(\Gamma_t)$ is generated by $\{4, \omega - 1\}$ and $\Lambda(\Gamma_8)$ is generated by $\{1, 4\omega\}$. There is one index 24 subgroup, Γ_r, which is a subgroup of Γ_t, and $\Lambda(\Gamma_r)$ is generated by $\{4, 2\omega - 2\}$. There are no index 48 subgroups contained in the index 6 subgroup.[5]

Now, we will show that there is no one-cusped congruence subgroup of $\mathcal{O}_3$-level (8). If Γ is such a group, $\Gamma\Gamma(4)$ must have $\mathcal{O}_3$-level (4) by the Ladder Lemma. Therefore, Γ must be a subgroup of one of the index 16 subgroups, Γ_8 or Γ_t. (since $\Gamma_r < \Gamma_t$). The group $\Gamma\Gamma(4)$ cannot be the index 16 subgroup. If it were, then $[\Gamma\Gamma(4) : \Gamma] = [\Gamma(4) : \Gamma \cap \Gamma(4)]$ which is 6 or 12, but $[\Gamma(4) : \Gamma \cap \Gamma(4)]$ divides 2^6. We check for low index subgroups of the images of these groups in $\mathrm{PSL}_2(\mathcal{O}_3)$ modulo N where N is the normal closure of the group generated by

$$\pm \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 8\omega \\ 0 & 1 \end{pmatrix}.$$

By Wohlfahrt's theorem, Λ of such a group must contain 8 and 8ω and not contain both 4 and 4ω. In Γ_8, we must check subgroups of index 2^b with $b \in \{1, 2, 3, 4\}$. There is one conjugacy class of index 2 subgroups, but Λ is generated by $\{2, 4\omega\}$, [5] therefore the $\mathcal{O}_3$-level of the corresponding group can be at most (4). As it is not conjugate to Γ_r, it is not a one-cusped congruence subgroup. There is one conjugacy class of index 4 subgroups, but it is a subgroup of the aforementioned index 2 subgroup [5] and therefore cannot be a one-cusped congruence subgroup. There are no index 8 subgroups, and there is one conjugacy class of index 16 subgroups with Λ is generated by $\{4, 4\omega\}$.[5] Therefore none of these are one-cusped of $\mathcal{O}_3$-level (8).

In Γ_t, there are 3 conjugacy classes of index 2 subgroups, one is Γ_r, the other two are one-cusped, but not congruence as can be seen by explicitly calculating the order of the group that they generate modulo (8) in $Mathematica^{TM}$. There is one conjugacy class of index 4 subgroups, a representative is contained in one of the above index 2 subgroups that is not conjugate to Γ_r[5] and therefore cannot be a one-cusped congruence subgroup. There are no index 8 subgroups.[5] Now assume that $[\Gamma_t : \Gamma] = 16$ and $\Gamma\Gamma(4) = \Gamma_t$. Since $1-\omega \in \Lambda(\Gamma\Gamma(4))$ and $\Gamma\Gamma(4) = \Gamma_t$, by the proof of the Ladder Lemma, $|\Lambda(\Gamma)| \leq 8 \cdot 4$ and $4-4\omega \in \Lambda(\Gamma)$, and so $[\mathrm{PSL}_2(\mathcal{O}_3) : \Gamma] \neq 3 \cdot 2^6$. Therefore, if $[\mathrm{PSL}_2(\mathcal{O}_3) : \Gamma] = 3 \cdot 2^6$, Γ must be an index 8 subgroup of $\Gamma_r = \Gamma\Gamma(4)$, but there are no index 8 subgroups of Γ_r modulo N. [5]

□

Lemma 4.3.6. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is inert and lies over 3. Then $T(\Gamma) = 2$, $d = 1$, and $n = 1$.*

Proof. **Case I:** $T(\Gamma) = 1$

As $\mathrm{PSL}_2(\mathbb{F}_9)$ has no index 3 or 9 subgroups, there is no one-cusped subgroup of $\mathcal{O}_d$-level (3). [5, 25] Assume Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level (9). Then

$$[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 3^a, a \in \{2, 3, 4\}$$

by the Index Lemma. There are no index 3,9, or 27 subgroups of $\mathrm{PSL}_2(\mathcal{O}_1)/N$ where N is the normal closure of the group generated by

$$\pm \begin{pmatrix} 1 & 9 \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 9\omega \\ 0 & 1 \end{pmatrix}.[5]$$

Therefore if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level (9), $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 81$. Since $\Gamma\Gamma(\mathcal{P}) = \mathrm{PSL}_2(\mathcal{O}_d)$, and therefore $[\Gamma\Gamma(\mathcal{P}) : \Gamma] = 3^4$ by the second isomorphism theorem, $\Gamma \cap \Gamma(\mathcal{P})$ is an index 3^4 subgroup of $\Gamma(\mathcal{P})$. As before since $\Gamma(\mathcal{P}^2) < \Gamma \cap \Gamma(\mathcal{P})$, $\Gamma \cap \Gamma(\mathcal{P})$ corresponds to a two-dimensional subspace F of $\Gamma(\mathcal{P})/\Gamma(\mathcal{P}^2)$. Let $v = (a, b, c)$ and $\nu = (\alpha, \beta, \gamma)$ be a basis for F with $a, b, c, \alpha, \beta, \gamma \in \mathbb{F}_9$. Since $\Lambda(\Gamma) =< 9, 9\omega >$, $(0, y, 0)$ or $(0, 0, y)$ are in F only when $y = 0$. If $a = \alpha = 0$ then we may assume that $b = 1$ and $\beta = w$, so $v = (0, 1, c)$ and $\nu = (0, \omega, \gamma)$. But, $M_{01} \cdot (-v) = (c, c, 1-c)$ implying that $c = 0$, which is not possible. Next assume that $a = 0$ but $\alpha \neq 0$. The generators are $(0, b, c)$ and (α, β, γ) with $b, c \neq 0$, and $M_{00} \cdot (0, b, c) = (0, c, b) \in F$ so $c = \pm b$. First, assume that $c = b$. Then $M_{01} \cdot (0, b, b) = (b, b, 0) \in F$. Acting on this by M_{00} gives $(b, 0, b) \in F$, and therefore $(0, b, -b) \in F$ which is not in the span. If $c = -b$, then $M_{12} \cdot (0, b, -b) = (0, 0, b) \in F$. Finally, we assume that both a and α are non-zero, so we have generators $(1, b, c)$ and (ω, β, γ). By acting on the generators with M_{00} we conclude that $b = c$ and $\beta = \gamma$. By acting on the first generator by M_{01} we see that $(1 + b, b, 1) \in F$ and therefore $b = 1$. But,

then $(2,1,1)$ and $(1,1,1)$ are in F implying that $(0,1,1) \in F$, which is not in the span. we conclude that if $T(\Gamma) = 1$, there are no one-cusped congruence subgroups of $\mathcal{O}_d$ level a power of (3).

Case II: $T(\Gamma) \neq 1$

Since $T(\Gamma) \neq 1$, $T = 2$ and $d = 1$. Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_1$-level (3). Then $[\mathrm{PSL}_2(\mathcal{O}_1) : \Gamma] = 6$ or 18. There is one conjugacy class of index 6 one-cusped congruence subgroups. [5] Also $\mathrm{PSL}_2(\mathbb{F}_9) \cong A_5$ which has no index 18 subgroups [5]. By the Ladder Lemma, it suffices to show that there are no one-cusped congruence subgroups of $\mathcal{O}_1$-level (9). Assume that Γ is such a subgroup. First, notice that $\Gamma\Gamma(3) \neq \mathrm{PSL}_2(\mathcal{O}_1)$. If this were the case, then as 2 divides $[\Gamma\Gamma(3) : \Gamma] = [\Gamma(3) : \Gamma \cap \Gamma(3)]$ then 2 divides $[\Gamma(\mathcal{P}) : \Gamma(\mathcal{P}^2)]$ by the second isomorphism theorem. But $[\Gamma(\mathcal{P}) : \Gamma(\mathcal{P}^2)] = 9^3$. Since 3^2 divides $4x$ by the Index Lemma,

$$x = [\mathrm{PSL}_2(\mathcal{O}_1) : \Gamma] \in \{2 \cdot 3^2, 2 \cdot 3^3, 2 \cdot 3^4\}.$$

The first case cannot occur because the index 6 subgroup has 1 conjugacy class of index 3 subgroups but the peripheral subgroup of one of these groups contains

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 3i \\ 0 & 1 \end{pmatrix} [5]$$

and so it cannot be one-cusped of $\mathcal{O}_1$-level (9) by Wohlfahrt's Theorem.

We now consider the case where $x = 2 \cdot 3^3$. The matrices M_{00}, M_{12}, M_{10}, M_{01}, and M_{11} are all contained in the index 6 subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ which must be $\Gamma\Gamma(3)$.[5] We will now proceed as before, letting F correspond to $\Gamma \cap \Gamma(3)$. When $x = 2 \cdot 3^3$, F is a 3^4-dimensional vector space over $\mathbb{F}_3$,

and $\Gamma \cap \Gamma(3)$ has $\{9, 3zi\}$ or $\{9i, 3z\}$ as generators for the peripheral lattice for $z \in \{1, 2\}$. We cannot say that $(0, y, 0)$ or $(0, 0, y)$ are in F only when $y = 0$. In fact, vectors of this form must be in F, but not both $(0, 1, 0)$ and $(0, i, 0)$, by Wolfahrt's theorem. Therefore there are basis vectors of the form (a, b, c), (α, β, γ), $(0, s, 0)$ and $(0, 0, s)$. In fact, by acting on the final vector with M_{01} we have $(-s, -s, s) \in F$, so we can assume the generators are (a, b, c), $(s, s, 0)$, $(0, s, 0)$ and $(0, 0, s)$. If $a = 0$, acting on the first generator by M_{01}, we conclude that $(-c, -c, -b+c) \in F$. Therefore we can assume that $c = s$, and $(s, s, b-s) \in F$, and so $(0, 0, b-s) \in F$ implying that $(0, 0, b) \in F$. But $M_{00} \cdot (0, 0, b) = (0, -b, 0) \in F$, and this implies that b is a multiple of s contradicting the linear independence of the basis.

Now assume that $a \neq 0$, so we assume that a is not a multiple of s. We may assume that $s = 1$ or $s = i$. In the first case, we may take $a = i$, with both b and c in $\{0, \pm i\}$. Acting on (a, b, c) by M_{00} we see that $b = c$. Acting on (i, b, b) by M_{01} gives $(i + b, b, i) \in F$ and so $b = i$, but then $(i, -i, -i) - (i, i, i) = (0, i, i) \in F$ which cannot occur. The case where $s = i$ is analogous.

If $x = 2 \cdot 3^4$, we have F corresponding to $\Gamma \cap \Gamma(\mathcal{P})$ as before. Here F is three-dimensional and we can conclude that $(0, 0, z)$ or $(0, z, 0)$ are in F only when $z = 0$, as $\Lambda(\Gamma)$ is generated by $\{9, 9i\}$. The generators are of the form

$$(1, a, b), (i, \alpha, \beta), (0, r, s) \text{ or } (a, 0, c), (0, 1, \beta), (0, i, s).$$

If it is the former, by acting by M_{00} we may assume that $r = s$ or $r = -s$. If $r = s$ after acting by M_{12} and M_{01} we see that $(r, -r, 0)$ and $(-r, -r, 0)$ are in F, and so $(0, r, 0) \in F$. If $r = -s$, then acting by M_{12} gives $(0, 0, r) \in F$.

In the latter case, $M_{12} \cdot (a, 0, c) = (-c, a + c, a + c) \in F$. Therefore, c is a multiple of a and $(a, 0, c)$ is $(a, 0, 0)$, $(a, 0, a)$ or $(a, 0, -a)$. In the first case, $M_{11} \cdot (a, 0, c) = (a, 0, -a) \in F$ and subtracting gives $(0, 0, a) \in F$. In the second case, $M_{12} \cdot (a, 0, 0) = (a, a, a) \in F$ and subtracting gives $(0, a, 0) \in F$. In the final case, $M_{00} \cdot (a, 0, -a) = (a - a, 0) \in F$ acting on this by M_{12} gives $(-a, -a, 0) \in F$ and therefore $(0, a, 0) \in F$.

□

4.3.3 Powers of Split Primes

Let p be a rational prime such that $\mathcal{P}_1$ and $\mathcal{P}_2$ lie over p. Let q_1 and q_2 be in $\mathcal{O}_d$ such that $(q_i) = \mathcal{P}_i$. We will now recall what we have proven thus far. We have shown in Proposition 4.0.2 that there are only one-cusped congruence subgroups of $\mathbb{Z}$-level p for $p \leq 11$. Assume that Γ is a one-cusped congruence subgroup of $\mathbb{Z}$-level p^n. By the Ladder Lemma, if $p > 3$, then $\Gamma\Gamma(p)$ has $\mathbb{Z}$-level p and hence $p \leq 11$. (If $p = 2$ or 3, the Ladder Lemma implies that $\Gamma\Gamma(p^2)$ has $\mathbb{Z}$-level p^2 if $n \geq 3$.) Also, by Lemma 4.2.2, if $p > 3$ we have seen that if the $\mathcal{O}_d$-level of Γ is p then $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^2$ and $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$. If $p = 3$ and Γ has $\mathcal{O}_d$-level p then either the index is $T(\Gamma)p^2$ and $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$ or the index is $T(\Gamma)p$.

Let Γ be a one-cusped congruence subgroup of $\mathbb{Z}$-level p^n where p is split. By above, $p \leq 11$. We will show that

$$n \leq \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } p = 5 \\ 1 & \text{if } p = 7 \text{ and } T(\Gamma) = 1 \\ 1 & \text{if } p = 11 \end{cases}$$

First, we will prove a structure lemma.

Lemma 4.3.7. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_1^{a_1}\mathcal{P}_2^{a_2}$ such that $a_i \geq 0$ and $a_1 \neq a_2$. Let $q_i \in \mathcal{O}_d$ be such that $(q_i) = \mathcal{P}_i$. Then $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^{a_1+a_2}$ and $\Lambda(\Gamma)$ is generated by $q_1^{a_1}q_2^{a_2}$ and $\omega(q_1^{a_1}q_2^{a_2})$.*

Next, we show

Lemma 4.3.8. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is split lying over p. Then unless $p = 7$ and $T(\Gamma) \neq 1$,*

$$n \leq \begin{cases} 4 & \text{if } p = 2 \\ 2 & \text{if } p = 3 \\ 1 & \text{if } 5 \leq p \leq 11. \end{cases}$$

Then we show

Lemma 4.3.9. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level (p^n) where p is split. Then unless $p = 7$ and $T(\Gamma) \neq 1$,*

$$n \leq \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } 5 \leq p \leq 11. \end{cases}$$

Finally, we show

Lemma 4.3.10. *Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_1^{a_1}\mathcal{P}_2^{a_2}$ where $a_2 \geq a_i$ and $\mathcal{P}_i$ lies over over p. Then unless $p = 7$ and $T(\Gamma) \neq 1$,*

$$a_2 \leq \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } 5 \leq p \leq 11 \end{cases}.$$

Lemma 4.3.8, 4.3.9, and 4.3.10 complete the proof of Proposition 4.0.3.

Proof of Lemma 4.3.7

First, consider the case where $a_2 = 0$. Since $\Gamma(\mathcal{P}_1^{a_1}) < \Gamma$, and $|\Lambda(\Gamma(\mathcal{P}_1^{a_1}))| = p^{a_1}$ we see that $|\Lambda(\Gamma)|$ divides p^{a_1}. If $p > 3$ then p^{a_1} divides $|\Lambda(\Gamma)|$ by the Index

Lemma, and so $\Lambda(\Gamma) = \Lambda(\Gamma(\mathcal{P}^{a_1}))$ and is generated by $\{q_1^{a_1}, \omega q_1^{a_1}\}$. If $p = 3$ one can check that if Γ has $\mathcal{O}_d$-level $\mathcal{P}_1^{a_1}$ that $\Gamma\Gamma(\mathcal{P}_1)$ has $\mathcal{O}_d$-level $\mathcal{P}_1$. Therefore $\Lambda(\Gamma)$ is generated by $\{q_1^{a_1}, \omega q_1^{a_1}\}$ here as well. Hence $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^{a_1}$.

Recall that if $\mathcal{R}$ is a split prime in $\mathcal{O}_d$ lying over r then as by assumption $\mathcal{O}_d$ is a PID, the split $(r) = \mathcal{R}_1\mathcal{R}_2$ arises as $\mathcal{R}_1 = (n + \omega)$, and $\mathcal{R}_2 = (n - \omega)$ where

$$-d \equiv n^2 \mod r.$$

So, $(n + \omega)(n - \omega) = ur$ where $u \in \mathcal{O}_d$ is a unit. And $(n + \omega)(n - \omega) \equiv 0 \mod r$, or alternately $(n + \omega)n \equiv \omega(n + \omega) \mod r$ and we see that

$$n\mathcal{R}_1 \equiv \omega\mathcal{R}_1 \mod r$$

where necessarily $(r, n) = 1$. Likewise,

$$-n\mathcal{R}_2 \equiv \omega\mathcal{R}_2 \mod r.$$

Let Γ be a one-cusped congruence group of $\mathcal{O}_d$- level $\mathcal{P}_1^{a_1}\mathcal{P}_2^{a_2}$ where $a_1 > a_2$. Recall that $\Lambda_x(\Gamma)$ is the minimal positive integer l such that

$$\begin{pmatrix} 1 & lx \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

First we will show that $\Lambda_1(\Gamma) = \Lambda_\omega(\Gamma) = p^{a_1}$. If $p^{a-1} \in \Lambda(\Gamma)$ then since $p^{a_2}q_1^{a_1-a_2} \in \Lambda(\Gamma)$,

$$p^{a_1-1}q_1^{a_1-a_2} = p^{a_1-1}(x + \omega y) \in \Lambda(\Gamma),$$

where $q_1^{a_1-a_2} = x + \omega y$ with $(p, x) = (p, y) = 1$. Since $p^{a_1-1} \in \Gamma$, $\omega y p^{a_1-1}$ and therefore $\omega p^{a_1-1} \in \Gamma$, and by Wohlfahrt's theorem, the $\mathbb{Z}$-level of Γ is p^{a_1-1}.

We have a similar contradiction if $\omega p^{a_1-1} \in \Lambda(\Gamma)$. Now from Section 3.4 we know that all elements in $\Lambda(\Gamma)$ are of the form

$$A\mathcal{D} + Bp^{a_1} + \omega Cp^{a_1}$$

where $\mathcal{D} = p^r(g + g'\omega)$. Since $p^{a_2}(x + \omega y) \in \Gamma$, any $Ap^r(g + g'\omega) \in \Gamma$ must have the property that

$$Ap^r(g + g'\omega) - Ep^r(x + \omega y) = B'p^{a_1} + \omega C'p^{a_1}$$

for some E when $r \geq a_2$. If there was some $Ap^r(g + g'\omega) + Bp^{a_1} + \omega Cp^{a_2} \in \Gamma$ where $r < a_2$, then $Ap^r(g + g'\omega) \in \Gamma$, so the lattice, Λ, generated by the elements $Ap^r(g+g'\omega)$, and p^{a_1} has width $Ag'p^{r+a_1}$. Therefore there is a lattice of width dividing p^{r+a_1} and the index of Γ can be at most p^{r+a_1}, which it is not. This shows that generators of the lattice are $\{q_1^{a_1-a_2}, p^{a_1}\}$, or $\{q^{a_1-a_2}, \omega p^{a_1}\}$. And,

$$[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^{a_1+a_2}.$$

This completes the proof

We would like to say something analogous about for the case when the $\mathcal{O}_d$- level is $\mathcal{P}_1^{a_1}\mathcal{P}_2^{a_1}$ but we cannot rule out the possibility that $\Lambda(\Gamma)$ has a proper diagonal as a generator.

Proof of Lemma 4.3.8

Let Γ be a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_d)$ of $\mathcal{O}_d$-level $\mathcal{P}^n$ where $\mathcal{P}$ is split and lies over p, and let

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma].$$

We will show that unless $p = 7$ and $T(\Gamma) \neq 1$ that

$$n \leq \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } 5 \leq p \leq 11 \end{cases}$$

For a congruence subgroup G of $\mathrm{PSL}_2(\mathbb{Z})$ we say that G has $\mathbb{Z}$-*level* n for $n \in \mathbb{N}$ if n is minimal with the property that the normal closure in $\mathrm{PSL}_2(\mathbb{Z})$, of the group generated by

$$\pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

is in G. Let Γ_z denote $\Gamma \cap \mathrm{PSL}_2(\mathbb{Z})$ and

$$x_z = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_z].$$

Notice that Γ_z is a congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ containing $\Gamma_z(p^n)$, the principal congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of $\mathbb{Z}$-level p^n, $\mathrm{PSL}_2(\mathbb{Z}) \cap \Gamma(\mathcal{P}^n)$. This implies that Γ_z has finite index in $\mathrm{PSL}_2(\mathbb{Z})$. One cannot a priori conclude that $\mathbb{H}^2/\Gamma_z$ has one cusp, or that the $\mathbb{Z}$-level of Γ_z is p^n, only that p^n divides the $\mathbb{Z}$-level of Γ_z. Let ϕ denote the modulo $\mathcal{P}^n$ map from $\mathrm{PSL}_2(\mathcal{O}_d)$ to $\mathrm{PSL}_2(\mathbb{Z}_{p^n})$. We will also use ϕ to denote the restriction of this map to $\mathrm{PSL}_2(\mathbb{Z})$. As such, the kernel of the restriction to $\mathrm{PSL}_2(\mathbb{Z})$ is $\Gamma_z(p^n)$.

Claim 4.3.11. *x_z divides x*

We will defer the proof of the claim and now complete the proof of Lemma 4.3.8 in the case where $T(\Gamma) = 1$. Both $\mathrm{PSL}_2(\mathcal{O}_d)$ and $\mathrm{PSL}_2(\mathbb{Z})$ surject $\mathrm{PSL}_2(\mathbb{Z}_{p^n})$ via ϕ as $\phi(\mathrm{PSL}_2(\mathbb{Z})) \cong \mathrm{PSL}_2(\mathbb{Z}_{p^n})$ and $|\mathrm{PSL}_2(\mathbb{Z}_{p^n})| = |\mathrm{PSL}_2(\mathcal{O}_d/\mathcal{P}^n\mathcal{O}_d)|$. Since $\Gamma_z < \Gamma$, x divides x_z and as we have shown that x_z divides x, we conclude that $\phi(\Gamma_z) = \phi(\Gamma)$ and

$$x = x_z = T(\Gamma)p^n.$$

Let

$$M_t = \pm \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

Notice that M_t is not contained in Γ for any $0 < t < p^n$ by Lemma 4.3.7. Thus the $\mathbb{Z}$-level of Γ_z is p^n. Every cusp of Γ_z corresponds to the same one-dimensional lattice, as the stabilizer of every cusp is conjugate. Therefore,

$$T(\Gamma)p^n = (\text{the cusp width of } \Gamma_z) \times (\text{the number of cusps of } \Gamma_z).$$

Since M_t is not in Γ_z for all $0 < t < p^n$, the cusp width of Γ_z is p^n. Therefore, if $T(\Gamma) = 1$, $\mathbb{H}^2/\Gamma_z$ has one cusp. We have also shown that Γ_z has $\mathbb{Z}$-level p^n. Therefore, in the case where $T(\Gamma) = 1$, the lemma follows by Petersson's result. [19]

If $T(\Gamma) \neq 1$ then $d = 1$ or 3. The only split prime of norm at most 11 in $\mathcal{O}_1$ lies over 5 and in $\mathcal{O}_3$ lies over 7. The case where $\mathcal{P}$ lies over 7 and $T(\Gamma) \neq 1$ is excluded in our hypothesis. Assume that $d = 1$, $p = 5$ and $T(\Gamma) = 2$. First assume Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}$. There is one conjugacy class of index 10, order 6 subgroups of $\mathrm{PSL}_2(\mathbb{F}_5)$, and any such group contains one conjugacy class of order 2 subgroups. [5] One representative of this conjugacy classs contains

$$\begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \equiv \begin{pmatrix} i & -1 \\ 0 & -i \end{pmatrix} \mod \mathcal{P}.[5]$$

This is a rotation of $2\pi/3$ about the $i/2$ axis. Moreover, one can verify that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Gamma = \begin{pmatrix} i & 4 \\ 0 & i \end{pmatrix} \Gamma,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Gamma = \begin{pmatrix} i & 2 \\ 0 & i \end{pmatrix} \Gamma,$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\Gamma = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}\Gamma,$$
$$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}\Gamma = \begin{pmatrix} i & 3 \\ 0 & i \end{pmatrix}\Gamma,$$
$$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}\Gamma = \begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix}\Gamma.$$

Therefore the pullback of any index 10 subgroup has 2 cusps, and any one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}$ has index 5 and has peripheral torsion. Now, assume that Γ has $\mathcal{O}_d$-level $\mathcal{P}^2$ and index 50. Modulo $\mathcal{P}^2$ $\phi(\Gamma)$ is an index 10 subgroup of $G = \phi(\Gamma\Gamma(\mathcal{P}))$, an index 5 subgroup in $\mathrm{PSL}_2(\mathbb{Z}_{25})$ Such a subgroup does not exist. [5]

Now we prove the claim, that x_z divides x.

Proof. First we will show that $\phi(\Gamma_z) = \phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}))$.

To see this it suffices to show that

$$\phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}) < \phi(\Gamma \cap \mathrm{PSL}_2(\mathbb{Z})).$$

If $\alpha \in \phi(\Gamma) \cap \phi(\mathrm{PSL}_2(\mathbb{Z}))$ we have $\alpha = \phi(\gamma) = \phi(\beta)$ for some $\gamma \in \Gamma \mathrm{and} \beta \in \mathrm{PSL}_2(\mathbb{Z})$. So, $\gamma \equiv \beta \mod \mathcal{P}^n$ and $\beta = \gamma M$ for some $M \in \Gamma(\mathcal{P}^n)$. Therefore $\beta \in \Gamma$ since $M \in \Gamma(\mathcal{P}^n) < \Gamma$ and therefore $\alpha = \phi(\beta)$ for $\beta \in \Gamma \cap \mathrm{PSL}_2(\mathbb{Z})$.

Notice that

$$|\phi(\Gamma_z)||\phi(\Gamma\mathrm{PSL}_2(\mathbb{Z}))| = |\phi(\Gamma)||\phi(\mathrm{PSL}_2(\mathbb{Z})|,$$

so

$$x_z = \frac{|\phi(\mathrm{PSL}_2(\mathbb{Z}))|}{|\phi(\Gamma_z)|} = \frac{|\phi(\Gamma\mathrm{PSL}_2(\mathbb{Z}))|}{|\phi(\Gamma)|}.$$

And

$$[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = \frac{|\phi(\mathrm{PSL}_2(\mathcal{O}_d))|}{|\phi(\Gamma)|} = \frac{|\phi(\mathrm{PSL}_2(\mathcal{O}_d))|}{|\phi(\Gamma \mathrm{PSL}_2(\mathbb{Z}))|} x_z.$$

□

Proof of Lemma 4.3.9

Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level (p^n). We will show that unless $p = 7$ and $T(\Gamma) = 1$,

$$n \leq \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } 5 \leq p \leq 11 \end{cases}.$$

We now recall some notation. Let

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma]$$

and

$$\phi' : \mathrm{SL}_2(\mathcal{O}_d) \to \mathrm{SL}_2(\mathbb{Z}_{p^n}) \times \mathrm{SL}_2(\mathbb{Z}_{p^n})$$

be the reduction modulo (p^n) map and let ρ_i be the projection into the i^{th} coordinate, the modulo $\mathcal{P}_i^n$ factor. If $\Gamma < \mathrm{PSL}_2(\mathcal{O}_d)$, then Γ' will be its $\mathrm{SL}_2(\mathcal{O}_d)$ pullback. Let $B_i' = \rho_i'(\phi'(\Gamma'))$ and

$$x_i = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_i^n)] = [\mathrm{SL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_i^n)'].$$

Case I: $5 \leq p \leq 11$**.**

We will show that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level (p^2), establishing the result by the Ladder Lemma. As $p > 3$, we conclude by Lemma 4.2.2 that $\Gamma\Gamma(p)$ has $\mathcal{O}_d$-level (p), index p^2 or $T(\Gamma)p^2$, and $\Gamma\Gamma(\mathcal{P}_1)$ and $\Gamma\Gamma(\mathcal{P}_2)$ have $\mathcal{O}_d$-levels $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. By the Index Lemma,

$x = T(\Gamma)p^k$ where $k = 2, 3$ or 4, but the above shows that $k \neq 2$. Assume that $T(\Gamma) = 1$, we will return to the case where $T(\Gamma) \neq 1$ shortly. Since there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}_i^2$, $\Gamma\Gamma(\mathcal{P}_i^2) = \Gamma\Gamma(\mathcal{P}_i)$ and

$$x_1 = [\mathrm{SL}_2(\mathcal{O}_d/\mathcal{P}_1^2) : B_1'] = p = [\mathrm{SL}_2(\mathcal{O}_d/\mathcal{P}_2^2) : B_2'] = x_2.$$

With N_i', a normal subgroup of B_i', defined as in Section 3.5, $[\mathrm{SL}_2(\mathcal{O}_d/\mathcal{P}_1^2) : N_1'] = x/x_2$ so

$$[B_1' : N_1'] = \frac{x}{x_1 x_2} = p \text{ or } p^2.$$

As a result, the abelianization of B_1' is divisible by p. But, if $p = 5$, there is one conjugacy class of index 5 subgroups in $\mathrm{PSL}_2(\mathbb{Z}_{25})$ with abelianization $\mathbb{Z}_3$. [5] If $p = 7$ there are two conjugacy classes of index 7 subgroups, each with abelianization $\mathbb{Z}_2$. [5] If $p = 11$ the abelianization of the index 11 subgroup is trivial. [5] So if $T(\Gamma) = 1$ and $5 \leq p \leq 11$ there are no one-cusped congruence subroups of $\mathcal{O}_d$-level (p^n) for $n \geq 2$.

Now assume that $d = 1$, $p = 5$ and $T(\Gamma) = 2$. If Γ has $\mathcal{O}_1$-level (p), then $x = 50$ and $x_i = 5$ by Lemma 4.2.2, so

$$[B_i' : N_i'] = \frac{x}{x_i^2} = \frac{50}{5^2} = 2.$$

However, the abelianization of any index 5 subgroup of $\mathrm{SL}_2(\mathbb{F}_5)$ is $\mathbb{Z}_3$. [5] So the only $\mathcal{O}_1$-level (5) subgroups have $T(\Gamma) = 1$ and index 25. If Γ has $\mathcal{O}_1$-level (5^2), and $T(\Gamma) = 2$ then $\Gamma\Gamma(5)$ has index 25, and $[\Gamma\Gamma(5) : \Gamma]$ =10 or 50. Also, $x_i = 5$, therefore

$$[N_i : B_i] = \frac{x}{x_i^2} = \frac{x}{5^2} = 10 \text{ or } 50$$

as $\Gamma\Gamma(\mathcal{P}_i^2) = \Gamma\Gamma(\mathcal{P}_i)$ and must be the index 5 subgroup. Any Sylow 5-subgroup of B_i' must be normal, so 5 must divide the abelianization of B_i', but it is $\mathbb{Z}_3$

so by the Ladder Lemma there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level (5^n) with peripheral torsion.

Case II: $p = 3$.

As $p = 3$, $d = 2$ or 11, so $T(\Gamma) = 1$. There are only one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}_i^n$ if $n \leq 2$ by Lemma 4.3.8. Let $q_i \in \mathcal{O}_d$ be such that $(q_i) = \mathcal{P}_i$. We may not a priori assume that if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_i^2$, that $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$. But in $\mathrm{PSL}_2(\mathbb{Z}_9)$ every conjugacy class of index 9 subgroups is a subgroup of an index 3 subgroup, (there is one conjugacy class of index 3 subgroups) and the coset representatives of the index 3 subgroup are conjugate to parabolic stabilizers of infinity so it has one cusp. [5] The index 3 subgroup corresponds to an $\mathcal{O}_d$-level $\mathcal{P}_i$ subgroup. Moreover, the index 9 subgroup can be shown to correspond to an $\mathcal{O}_d$-level (9) subgroup. Therefore by Lemma 4.2.2 if Γ has $\mathcal{O}_d$-level (9) then $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$.

By the Index Lemma, if Γ is a one-cusped congruence subgroup of $\mathcal{O}_d$-level (3^2), then

$$x = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 3^2, 3^3, \text{ or } 3^4.$$

We will show that it is 3^4. First, we will show that $x \neq 3^2$. If $x = 3^2$, $\Gamma\Gamma(\mathcal{P}_i^2)$ cannot have $\mathcal{O}_d$-level $\mathcal{P}_i^2$ as then $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_i)] = p^2$ and so cannot be properly contained in Γ. If $\Gamma\Gamma(\mathcal{P}_i^2)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$ then $\Lambda(\Gamma\Gamma(\mathcal{P}_i)) = \{q_i, \omega q_i\}$, and $[\Gamma\Gamma(\mathcal{P}_i) : \Gamma] = 3$ so $\{3q_i, 3\omega q_i\} \subset \Lambda(\Gamma)$, and we conclude that the $\mathcal{O}_d$-level of Γ divides $(3\mathcal{P}_i)$. Therefore $\Gamma\Gamma(\mathcal{P}_i) = \mathrm{PSL}_2(\mathcal{O}_d)$ and

$$[B_2' : N_2'] = [\mathrm{SL}_2(\mathcal{O}_d/(n_2)) : N_2'] = \frac{x}{x_1} = 3^2.$$

Therefore after projectivizing we see that 9 must divide the order of the abelianization of $\mathrm{PSL}_2(\mathbb{Z}_9)$, but it is $\mathbb{Z}_3$. [5]

Now assume that $x = 3^3$, so

$$x_i = [\mathrm{SL}_2(\mathbb{Z}_9) : B_i'] = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}_i)] = 1, 3, \text{ or } 3^2$$

and

$$[\mathrm{SL}_2(\mathbb{Z}_9) : N_2'] = 3^3/x_1.$$

If $x_1 = 1$, then $[\mathrm{SL}_2(\mathbb{Z}_9) : N_2'] = 3^3$. Therefore $x_2 \neq 3$ or 3^2 as the abelianization of any subgroup of index 3 or 3^2 of $\mathrm{PSL}_2(\mathbb{Z}_9)$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$. [5] So $x_2 = 1$ and N_1 is a normal index 27 subgroup of $\mathrm{PSL}_2(\mathbb{Z}_9)$. But there are no normal index 27 subgroups in $\mathrm{PSL}_2(\mathbb{Z}_9)$. [5] If $x_1 = 3$ then $[\mathrm{SL}_2(\mathbb{Z}_9) : N_2'] = 3^2$. Therefore $x_2 \neq 1$ or 3 as there are no normal subgroups of $\mathrm{PSL}_2(\mathbb{Z}_9)$ of index 9, and the abelianization of any index 3 subgroup is $\mathbb{Z}_2 \times \mathbb{Z}_2$. So $x_2 = 3^2$. But notice that $\Gamma\Gamma(\mathcal{P}_i)$ has $\mathcal{O}_d$-level $\mathcal{P}_i$, so $\Gamma\Gamma(\mathcal{P}_1) \cap \Gamma\Gamma(\mathcal{P}_2) = \Gamma\Gamma(3)$, which has $\mathcal{O}_d$-level (3). Since $x = 3^3$, Γ is an index 3 subgroup of both $\Gamma\Gamma(3)$ and $\Gamma\Gamma(\mathcal{P}_2^2)$, one-cusped congruence subgroups of $\mathcal{O}_d$-level (3) and $\mathcal{P}_2^2$, respectively. But this is impossible as $\Lambda(\Gamma\Gamma(3)) = \{3, 3\omega\}$ and $\Lambda(\Gamma\Gamma(\mathcal{P}_2^2)) = \{q_2^2, \omega q_2^2\}$. Finally, if $x_1 = 3^2$ then we obtain a contradiction as above, since $\{q_1^2, \omega q_1^2\}$ is contained in $\Lambda(\Gamma)$.

Therefore $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 3^4$. We will now figure out the subgroup diagram of this group. We have

$$[\mathrm{SL}_2(\mathcal{O}_d/(n_2)) : N_2'] = 3^4/x_1$$

and

$$[SL_2(\mathcal{O}_d/(n_1)) : N_1'] = 3^4/x_2.$$

If $x_1 = 1$ then the index of N_2' is 3^4. Recall that $N_2' \triangleleft B_2'$, as a result x_2 cannot be 3 or 3^2 as the abelianization of the index 3 and 9 subgroups of $\mathrm{SL}_2(\mathbb{Z}_9)$ are all $\mathbb{Z}_2 \times \mathbb{Z}_2$. [5] But x_2 cannot be 1 as there are no normal index 81 subgroups of $\mathrm{PSL}_2(\mathbb{Z}_9)$,[5] therefore $x_1 \neq 1$. If $x_1 = 3$, the index of N_2' is 3^3, x_2 cannot be 1 as there are no normal subgroups of $\mathrm{PSL}_2(\mathbb{Z}_9)$ of index 27.[5] Also, x_2 canot be 3 or 3^2 as the abelianization of the index 3 and 9 subgroups are $\mathbb{Z}_2 \times \mathbb{Z}_2$.[5] So $x_i = 3^2$. We have $\Gamma\Gamma(\mathcal{P}_i)$ of $\mathcal{O}_d$-level $\mathcal{P}_i$, so we deduce that $\Gamma\Gamma(3)$ has $\mathcal{O}_d$-level (3) and index 3^2. Also, we know that $\Gamma\Gamma(\mathcal{P}_i^2)$ has $\mathcal{O}_d$-level $\mathcal{P}_i^2$.

Now we are ready to show that there is no one-cusped congruence subgroup of $\mathcal{O}_d$-level (3^3). Assume that Γ is such a group. Then $\Gamma\Gamma(3^2)$ has $\mathcal{O}_d$-level (3^2). Therefore $[\Gamma\Gamma(3^2) : \Gamma] = 3$ or 3^2 since $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(\mathcal{P}^2)] = 81$. First assume it is 3. So

$$[\mathrm{SL}_2(\mathcal{O}_d/(n_i)) : N_i'] = \frac{3^5}{x_2} = 3^3$$

and therefore

$$[B_i' : N_i'] = 3.$$

But, in $\mathrm{SL}_2(\mathbb{Z}_{27})$ the abelianization of an index 9 subgroup is $\mathbb{Z}_2 \times \mathbb{Z}_2$ [5]. Now we may assume Γ is as above of index 3^6. In this case we see that $[\mathrm{SL}_2(\mathcal{O}_d/(n_2)) : N_2'] = 3^4$ and so $[B_i' : N_i'] = 3^2$ implying that the index 9 subgroup has abelianization $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$. We conclude that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level (3^n) when $n > 2$.

Proof of Lemma 4.3.10

Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$-level $\mathcal{P}_1^{a_1}\mathcal{P}_2^{a_2}$ with $a_2 \geq a_1$. We will show that unless $p = 7$ and $T(\Gamma) \neq 1$ that

$$a_2 \leq \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } 5 \leq p \leq 11 \end{cases}.$$

By the Ladder Lemma, if $p > 3$ and $a_1 > 1$ then $\Gamma\Gamma(\mathcal{P}_1\mathcal{P}_2)$ has $\mathbb{Z}$-level p. Therefore $p \leq 11$ by Proposition 4.0.2. If $5 \leq p \leq 11$ then $\Gamma\Gamma(\mathcal{P}_1^2\mathcal{P}_2^2)$ has $\mathbb{Z}$-level p^2. From Lemma 4.3.9, the $\mathcal{O}_d$-level cannot be (p^2), and from Lemma 4.3.8 it cannot be $\mathcal{P}_i^2$. So it suffices to show that there are no one-cusped congruence subgroups of $\mathcal{O}_d$-level $\mathcal{P}_1^2\mathcal{P}_2$. Similarly, if $p = 3$ it suffices to rule out the existence of such groups of $\mathcal{O}_d$-level $\mathcal{P}_1^3\mathcal{P}_2$ and $\mathcal{P}_1^3\mathcal{P}_2^2$.

First, assume that Γ has $\mathcal{O}_d$-level $\mathcal{P}_1^2\mathcal{P}_2$ and $5 \leq p \leq 11$. By Lemma 4.3.7, $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = T(\Gamma)p^3$. Also $[\mathrm{SL}_2(\mathbb{Z}_{p^2}) : N_1'] = T(\Gamma)p^3/x_2$ with $x_2 = 1$ or p. But this implies that p^2 divides $|\mathrm{SL}_2(\mathbb{Z}_p)|$ which is not the case.

Now assume that $p = 3$ and Γ has $\mathcal{O}_d$-level $\mathcal{P}_1^3\mathcal{P}_2$. Recall that $T(\Gamma) = 1$. By Lemma 4.3.7 $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 3^4$ and $[\mathrm{SL}_2(\mathbb{Z}_{3^3}) : N_1'] = 3^4/x_2$ with $x_2 = 1$ or 3, again implying that 3^2 divides $|\mathrm{SL}_2(\mathbb{Z}_3)|$. If the $\mathcal{O}_d$-level of Γ is $\mathcal{P}_1^3\mathcal{P}_2^2$ then the index is 3^5. Notice that $|\mathrm{SL}_2(\mathbb{Z}_{3^2})| = 3^4 2^3$. Therefore $[\mathrm{SL}_2(\mathcal{O}_d/(n_2)) : N_2'] \neq 3^5$, implying that $x_1 \neq 1$. So

$$[\mathrm{SL}_2(\mathcal{O}_d/(n_2)) : N_2'] = \frac{3^5}{x_1} = 3^4 \text{ or } 3^3.$$

If $x_2 = 3$ then $[B_2' : N_2'] = 3^3$ or 3^2, but the abelianization of any index 3 subgroup is $\mathbb{Z}_2 \times \mathbb{Z}_2$.[5] If $x_2 = 3^2$, then $[B_2' : N_2'] = 3^2$ or 3, but the abeilanization of the index 9 subgroup is also $\mathbb{Z}_2 \times \mathbb{Z}_2$.[5] Therefore $x_2 = 1$ and

since $x_1 \neq 1$,

$$[\mathrm{SL}_2(\mathcal{O}_d/(n_1)) : N_1'] = \frac{x}{x_2} = 3^5$$

and $[B_1' : N_1'] = 3^4$ or 3^3. But the abelianization of the index 3 or 9 subgroup in $\mathrm{SL}_2(\mathbb{Z}_{27})$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$.[5]

Chapter 5

Proof of Corollary 1.1.2

To prove the corollary it is enough to show that 6 does not divide the index $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma]$ for any one-cusped congruence subgroup, Γ. [10]

Table 5.1:
Splitting Types of Small Primes in $\mathcal{O}_d$, R=Ramified, S=Split and I=Inert

	$d=1$	2	3	7	11	19	43	67	163
$p=2$	R	R	I	S	I	I	I	I	I
3	I	S	R	I	S	I	I	I	I
5	S	I	I	I	S	S	I	I	I
7	I	I	S	R	I	S	I	I	I
11	I	S	I	S	R	S	S	I	I

If $p \in \mathbb{Z}$ is prime, and inert or ramified, let $\mathcal{P}_p$ denote the prime lying over p. If p is split, then we will write $(p) = \mathcal{P}_p\mathcal{Q}_p$. Recall some notation from Section 3.5. Let Γ be a one-cusped congruence subgroup of $\mathcal{O}_d$ level (n), let

$$x = [\mathrm{PSL}_2(\mathcal{O}_d : \Gamma]$$

For n_1 and n_2 such that $(n_1, n_2) = \mathcal{O}_d$ and $(n_1) \cap (n_2) = (n)$, let

$$x_i = [\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma\Gamma(n_i)],$$

and let $M(m) = |\mathrm{SL}_2(\mathcal{O}_d/(m))|$ for all non-zero $(m) \subset \mathcal{O}_d$. Recall that

$$|N_2'| = \frac{x_1 M(n_2)}{x} \in \mathbb{Z}.$$

5.1 $\mathrm{PSL}_2(\mathcal{O}_{43})$

We have seen in Lemma 4.1.2 that there can be no one-cusped congruence subgroup of $\mathcal{O}_{43}$-level $\mathcal{P}_3^{a_3}\mathcal{P}_2^{a_2}$ unless $a_3 = 0$. Suppose that $(n) = \mathcal{P}_2^{a_3}\mathcal{P}_{11}^{a_{11}}$, and let $(n_1) = \mathcal{P}_2^{a_3}$ and $(n_2) = \mathcal{P}_{11}^{a_{11}}$. Since $x_1 = 1$ and

$$|N_2'| = \frac{x_1 M(n_2)}{x} = \frac{11 \cdot 5 \cdot 3 \cdot 2^3}{x}$$

we conclude that 3^2 does not divide x and therefore $a_3 = 1$. Therefore $[\mathrm{SL}_2(\mathbb{F}_9) : N_1'] = x/x_2$ which must be 3. This implies that N_1 is a proper normal subgroup of $\mathrm{PSL}_2(\mathbb{F}_9)$. Similarly, since 3^2 does not divide $M(\mathcal{P}_2)$, $M(\mathcal{P}_{11})$ or $M(\mathcal{Q}_{11})$, one can show that (n) cannot be a product of a power of $\mathcal{P}_3$ and powers of two other primes, and then one can show that (n) cannot be a product of a power of $\mathcal{P}_3$ and powers of all $\mathcal{P}_2$, $\mathcal{P}_{11}$ and $\mathcal{Q}_{11}$.

Since 11 does not divide $M(\mathcal{P}_2)$, as above, we can show that 11^2 cannot divide the $\mathbb{Z}$-level.

If $(n) = \mathcal{P}_{11}\mathcal{P}_2^{a_2}$ then let $(n_1) = \mathcal{P}_{11}$ and $(n_2) = \mathcal{P}_2^{a_2}$. Recall that $x_2 = 1$ or 16, and $x_1 = 11$. Therefore $[B_1' : N_1'] = x/11$ or $x/(11 \cdot 16)$, which is a power or 2 in either case. But any such B_1' has trivial abelianization [5], so either $x = 11$ or $x = 16 \cdot 11$. The first case cannot occur if $a_2 > 1$ and the second case occurs if $\Gamma\Gamma(\mathcal{P}_2)$ has $\mathcal{O}_{43}$-level $\mathcal{P}_2^2$ and index 16, implying that the Ox_{43}-level of Γ is $\mathcal{P}_{11}\mathcal{P}_2^2$.

The case where $(n) = \mathcal{P}_{11}\mathcal{Q}_{11}Px_2^{a_2}$ is similar.

Lemma 5.1.1. *If Γ is a one-cusped congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_{43})$ then the $\mathcal{O}_{43}$-level is one of the following:*

$$\mathcal{P}_{11}, \mathcal{Q}_{11}, \mathcal{P}_{11}\mathcal{Q}_{11}, \mathcal{P}_2^2, \mathcal{P}_2^2\mathcal{P}_{11}, \mathcal{P}_2^2\mathcal{Q}_{11}, \mathcal{P}_2^2\mathcal{P}_{11}\mathcal{Q}_{11}.$$

Moreover, Γ *contains torsion.*

5.2 $\mathrm{PSL}_2(\mathcal{O}_{67})$ and $\mathrm{PSL}_2(\mathcal{O}_{163})$

For these values of d, all of 2, 3, 5, 7 and 11 are inert. By Lemma 4.1.2 we conclude

Lemma 5.2.1. *If* Γ *is a one-cusped congruence subgroup of* $\mathrm{PSL}_2(\mathcal{O}_d)$ *where* $d = 67$ *or 163 then* $[\mathrm{PSL}_2(\mathcal{O}_d) : \Gamma] = 16$ *and the* $\mathcal{O}_d$*-level of* Γ *is* (4)*. Moreover,* Γ *contains torsion.*

5.3 $\mathrm{PSL}_2(\mathcal{O}_{19})$

Here 2 and 3 are inert and 5,7 and 11 are split. Since 3^2 does not divide $M(\mathcal{P}_2)$, $M(\mathcal{P}_5)$, $M(\mathcal{Q}_5)$, $M(\mathcal{P}_7)$, $M(\mathcal{Q}_7)$, $M(\mathcal{P}_{11})$ or $M(\mathcal{Q}_{11})$ we conclude as above the $\mathcal{P}_3$ does not divide the $\mathcal{O}_{19}$ level. Since 11^2 does not divide $M(\mathcal{P}_2)$, $M(\mathcal{P}_5)$, $M(\mathcal{Q}_5)$, $M(\mathcal{P}_7)$, or $M(\mathcal{Q}_7)$ we conclude that 11^2 does not divide the $\mathbb{Z}$-level. Likewise, we conclude that neither 5^2 nor 7^2 divide the $\mathbb{Z}$-level. We can bound the power of $\mathcal{P}_2$ dividing the $\mathbb{Z}$-level by 25, but most likely there is a more modest bound. As a consequence

Lemma 5.3.1. *The* $\mathbb{Z}$*-level of a one-cusped congruence subgroups of* $\mathcal{O}_{19}$ *divides*

$$11^2 7^2 5^2 2^{25}.$$

All one-cusped congruence subgroups of $\mathcal{O}_{19}$ *have torsion.*

Chapter 6

Proof of Theorem 1.1.4

We will prove Theorem 1.1.4, which states that if K is either $\mathbb{Q}$ or an imaginary quadratic number field with class number one, then there are infinitely many maximal congruence subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$ that have two cusps. Moreover, for any even integer n, there are infinitely many primes $\mathcal{P} \subset \mathcal{O}_K$ such that there is an n-cusped congruence subgroup of $\mathcal{O}_K$-level $\mathcal{P}$.

First, we will prove the theorem for $K = \mathbb{Q}$. Let p be an odd prime and let ϕ denote the modulo p map from $\mathrm{PSL}_2(\mathbb{Z})$ to $\mathrm{PSL}_2(\mathbb{F}_p)$. By the classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$ there is a maximal subgroup, H, of index $p+1$. [25] Since p is odd,

$$\Gamma(p) = \{M \in \mathrm{PSL}_2(\mathbb{Z}) : M \equiv I \mod p\}$$

has $(p^2-1)/2$ cusps all of width p. Let $\Gamma = \phi^{-1}(H)$. This has two cusps by Wohlfahrt's theorem, one of width one and one of width p.

The group H has a normal Sylow p-subgroup, S, and the quotient of H by S is cyclic of order $(p-1)/2$. [25] The group $\Gamma(p)$ has $(p^2-1)/2$ cusps, all of width p. As p does not divide $(p-1)/2$, the cusp of width one in $\phi^{-1}(H)$ must lift to $(p-1)/2$ cusps of width one in $\phi^{-1}(S)$. Therefore the cusp of

width p must lift to $(p-1)/2$ cusps of width p in $\phi^{-1}(S)$. So $\phi^{-1}(S)$ has $p-1$ cusps. If l divides $(p-1)/2$ there is a subgroup L such that $S < L < H$ and $[H : L] = l$. The preimage, $\phi^{-1}(L)$ has l cusps of width one and l of width p, for a total of $2l$ cusps. Therefore we have subgroups of $\mathbb{Z}$-level p with $2l$ cusps for all divisors, l, of $(p-1)/2$. For a fixed even t, there are infinitely many primes p such that $p \equiv 1 \mod t$, and as a result we have infinitely many maximal t-cusped subgroups.

Let $K = \mathbb{Q}(\sqrt{-d})$ for $d \in \{2, 7, 11, 19, 43, 67, 163\}$. Let $\mathcal{P}$ be a prime in $\mathcal{O}_d$, such that $q = N(\mathcal{P})$ is odd. If $A < \mathrm{PSL}_2(\mathbb{F}_q)$ and the pre-image of A has n-cusps, we will say that A has n cusps. If $\mathcal{P}$ is split, lying over p then we analyze the quotient $\mathrm{PSL}_2(\mathcal{O}_d)$ by $\Gamma(\mathcal{P})$ and as above conclude that H has two cusps and for all even divisors, t, of $(p-1)$ there is a subgroup L of $\mathrm{PSL}_2(\mathbb{F}_p)$ such that L has $t/2$ cusps of width one and $t/2$ cusps of width p, for a total of t cusps.

Now consider the case where p is inert, so the quotient is $\mathrm{PSL}_2(\mathbb{F}_{p^2})$. As above there is an index p^2+1 subgroup, H, and H has a normal Sylow p-subgroup, S. The quotient H/S is cyclic of order $(p^2-1)/2$. [25] There are two possibilities for cusps of H. First, H may have A cusps of width one and B cusps of width p. Second, H may have one cusp of width one and one cusp of width p^2. We will show that the first case cannot occur. Recall that $\Gamma(\mathcal{P})$ has $(p^4-1)/2$ cusps of width p^2, and $\mathrm{PSL}_2(\mathcal{O}_d)$ has one cusp of width one. The subgroup $S < H$ has k cusps of width 1, l cusps of width p and m of width p^2. As $S \triangleleft H$, and $[H : S] = (p^2-1)/2$, in the covering corresponding to $S < H$, one of the B cusps of H of width one must be covered by cusps of S which all

of the same width. As a result, since p does not divide the covering degree, we conclude that such a cusp is covered by width one cusps, and $k = B(p^2-1)/2$. Similarly, for a cusp of H of width p, it must be covered by only cusps of width p, and hence $l = A(p^2-1)/2$. Now consider the covering corresponding to $\{id\} < S$. A cusp of width one in S, is covered by one cusp of width p^2 in $\{id\}$, and a cusp of width p is covered by p cusps of width p^2. Since there are $(p^4-1)/2$ cusps in $\{id\}$ this implies that

$$\frac{Ap^2(p^2-1)}{2} + \frac{Bp(p^2-1)}{2} = \frac{p^4-1}{2}$$

which cannot occur.

Therefore H has one cusp of width one and one cusp of width p^2. Since $S \triangleleft H$, and $[H : S] = (p^2-1)/2$ we conclude that the cusp of with one in H is covered by $(p^2-1)/2$ cusps of width one in S, as all of the covers must have the same width. Therefore the cusp of width p^2 is covered by $(p^2-1)/2$ cusps of width p^2. We conclude that S has $(p^2-1)/2$ cusps of width one and $(p^2-1)/2$ of width p^2. As H/S is cyclic of order $(p^2-1)/2$, for any l dividing $(p^2-1)/2$, there is a subgroup L of H of index l which has l cusps of width one and l of width p^2, for a total of $2l$ cusps.

Therefore, combining the split and inert cases, given an even t, we need only show that there are infinitely many primes $\mathcal{P} \subset \mathcal{O}_d$ with

$$N(\mathcal{P}) \equiv 1 \mod t.$$

By Dirichlet's Theorem on primes in an arithmetic progression, there are infinitely many primes $p \in \mathbb{Z}$ such that $p \equiv 1 \mod t$. [26] For any $\mathcal{P}$ lying over p, $N(\mathcal{P}) = p$ or p^2 and therefore $N(\mathcal{P}) \equiv 1 \mod t$ as well.

Now consider the case where $d = 1$ or 3. Notice that in $\mathcal{O}_1 = \mathbb{Z}[i]$, a prime p splits when $p \equiv 1 \mod 4$ and is inert if $p \equiv -1 \mod 4$. In $\mathcal{O}_3 = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ a prime p splits when $p \equiv 1 \mod 6$ and p is inert when $p \equiv -1 \mod 6$. This is due to the fact that both are cyclotomic extensions. In $\mathcal{O}_1$, consider a split prime, p, lying under $\mathcal{P}$ and the quotient $\mathrm{PSL}_2(\mathbb{F}_p)$. Here $\{id\}$ has $(p^2-1)/4$ torsion-free cusps, all of width p. Since $|S| = p$, we conclude that all cusps of S are torsion-free and S has $(p-1)/4$ cusps of width one and $(p-1)/4$ of width p. As before, we conclude that H has one cusp (with torsion) of width one and one cusp (with torsion) of width p. Since $\phi^{-1}(S)$ is peripheral torsion-free, there is a representative of peripheral torsion in the cyclic quotient H/S. Let T be the group such that $S < T < H$ which corresponds to that quotient, so $[T : S] = 2$. Therefore, T has $(p-1)/4$ cusps of with one and $(p-1)/4$ of width p, all of which have torsion. As above, for any l dividing $(p-1)/4$ we have a subgroup of H containing T with $2l$ cusps. Since for any even t, there are infinitely many primes $p \in \mathbb{Z}$ with $p \equiv 1 \mod 2t$, these primes split and the $\mathrm{PSL}_2(\mathbb{F}_p)$ have subgroups with t cusps. So, there is a subgroup of $\mathrm{PSL}_2(\mathcal{O}_1)$ containing $\Gamma(\mathcal{P})$ with t cusps, $t/2$ of width one and $t/2$ of width p. Similarly, for $\mathcal{O}_3$ for a given even t, as there are infinitely many primes $p \in \mathbb{Z}$ with $p \equiv 1 \mod 3t$, these primes split and the $\mathrm{PSL}_2(\mathbb{F}_p)$ have subgroups with t cusps.

Bibliography

[1] M. D. Baker and A. W. Reid. In preparation.

[2] M. D. Baker and A. W. Reid. Arithmetic knots in closed 3-manifolds. *J. Knot Theory Ramifications*, 11(6):903–920, 2002. Knots 2000 Korea, Vol. 3 (Yongpyong).

[3] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geq 3)$ and $\mathrm{Sp}_{2n}\,(n \geq 2)$. *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[4] A. M. Brunner, M. L. Frame, Y. W. Lee, and N. J. Wielenberg. Classifying torsion-free subgroups of the Picard group. *Trans. Amer. Math. Soc.*, 282(1):205–235, 1984.

[5] J. Cannon. *Magma*. University of Sydney, 2000.

[6] T. Chinburg, D. Long, and A. W. Reid. Cusps of minimal non-compact arithmetic hyperbolic orbifolds. *In preparation*.

[7] B. Fine. *Algebraic theory of the Bianchi groups*, volume 129 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1989.

[8] R. Fricke. Über die substitutionsgruppen welche zu den aus dem legendreschen integralmodul gezogenen wurzeln gehoren. *Math Annalen*, (28):99–118, 1886.

[9] P. M. Gruber and C. G. Lekkerkerker. *Geometry of numbers*, volume 37 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, second edition, 1987.

[10] F. Grunewald and J. Schwermer. Subgroups of Bianchi groups and arithmetic quotients of hyperbolic 3-space. *Trans. Amer. Math. Soc.*, 335(1):47–78, 1993.

[11] C. J. Leininger. Compressing totally geodesic surfaces. *Topology Appl.*, 118(3):309–328, 2002.

[12] H. W. Lenstra, Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.*, 42:201–224, 1977.

[13] A. Lubotzky. Free quotients and the congruence kernel of SL_2. *J. Algebra*, 77(2):411–418, 1982.

[14] D. A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[15] J. L. Mennicke. Finite factor groups of the unimodular group. *Ann. of Math. (2)*, 81:31–37, 1965.

[16] Th. Motzkin. The Euclidean algorithm. *Bull. Amer. Math. Soc.*, 55:1142–1146, 1949.

[17] M. Newman. *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[18] H. Petersson. Über einen einfachen Typus von Untergruppen der Modulgruppe. *Arch. Math.*, 4:308–315, 1953.

[19] H. Petersson. Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe. *J. Reine Angew. Math.*, 250:182–212, 1971.

[20] G. Pick. *Ü*ber gewisse ganzzahlige lineare substitutionen welche sich nicht durch algebraisches congruenzen erklaren lassen. *Math. Annalen*, (28):119–124, 1886.

[21] A. W. Reid. Arithmeticity of knot complements. *J. London Math. Soc. (2)*, 43(1):171–184, 1991.

[22] P. Samuel. About Euclidean rings. *J. Algebra*, 19:282–301, 1971.

[23] J.-P. Serre. Le problème des groupes de congruence pour SL2. *Ann. of Math. (2)*, 92:489–527, 1970.

[24] J. G. Sunday. Presentations of the groups SL(2, m) and PSL(2, m). *Canad. J. Math.*, 24:1129–1131, 1972.

[25] M. Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

[26] H. P. F. Swinnerton-Dyer. *A brief guide to algebraic number theory*, volume 50 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2001.

[27] G. van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

Vita

Kathleen Lizabeth Petersen was born in Abington, Pennsylvania, on February 24, 1976 to Albert and Christine Petersen. She graduated from Abington High School in 1994 and then attended Oberlin College, receiving a B.A. in Mathematics in 1998. In August 1999 she entered the Graduate School of the University of Texas at Austin.

Permanent address: 301 East 34th Street #101
Austin, Texas 78705

This dissertation was typeset with LaTeX‡ by the author.

‡LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.